NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

FORCENET: AN ANALYSIS OF THE TRIDENT WARRIOR 2003 EXERCISE

by

John P. Lagana Jr.

September 2004

Thesis Advisor:	Dan C. Boger
Second Reader:	Susan Higgins

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** September 2004	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE: FORCEnet: An Analysis of the Trident Warrior 2003 Exercise			**5. FUNDING NUMBERS**
6. AUTHOR(S) John P. Lagana			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited			**12b. DISTRIBUTION CODE**

13. ABSTRACT (maximum 200 words)

Since the country has moved into the Information Age, the military forces have been moving towards network based operations. The rapid expansion of the internet and information technology (IT) has led to the emerging theory of Network-Centric Warfare (NCW). The Naval Services instantiation of NCW is FORCEnet. "FORCEnet is the "glue" that binds together Sea Strike, Sea Shield, and Sea Basing. It is the operational construct and architectural framework for naval warfare in the Information Age, integrating warriors, sensors, command and control, platforms, and weapons into a networked, distributed combat force. FORCEnet will provide the architecture to increase substantially combat capabilities through aligned and integrated systems, functions, and missions.

Sea Power 21 is a comprehensive attempt to address the ramifications of the Information Age revolution. The framework of the Sea Power 21 vision is composed of the following elements: Sea Basing, Sea Shield and Sea Strike. The enabler of this vision or the "glue" that holds it all together is FORCEnet. FORCEnet is "the operational construct and architectural framework of naval warfare in the information age that integrates Warriors, sensors, networks, command and control, platforms, and weapons into a networked, distributed combat force that is scaleable across all levels of conflict from seabed to space and sea to land."

The Trident Warrior 03 exercise was then developed as a means to measure its success and to acquire data from which future exercises can be measured against. FORCEnet is still in its infancy and many people have different views on what exactly it is and how it should be implemented to achieve those goals. The intent of this thesis was not to answer those questions per se, but provide a realistic analysis of what worked during the TW03 exercise and what did not. This should provide a baseline for further Trident Warrior exercises so as to avoid the same mistakes in the future. The military has a ways to go before it can fully realize a truly networked-centric armed forces, but TW03 was the beginning and the lessons learned from it will pay dividends in realizing that fully networked goal.

14. SUBJECT TERMS Network Centric Warfare, Information Warfare, FORCEnet, Trident Warrior, Joint Vision 2020, Sea Power 21			**15. NUMBER OF PAGES** 95
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UL

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

FORCENET: AN ANALYSIS OF THE TRIDENT WARRIOR 2003 EXERCISE

John P. Lagana Jr.
Major, United States Marine Corps
B.S., Purdue University, 1992

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN INFORMATION TECHNOLOGY MANAGEMENT

from the

NAVAL POSTGRADUATE SCHOOL
September 2004

Author: John P. Lagana Jr.

Approved by: Dan C. Boger
Thesis Advisor

Susan Higgins
Second Reader

Dan C. Boger
Chairman, Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Since the country has moved into the Information Age, the military forces have been moving towards network based operations. The rapid expansion of the internet and information technology (IT) has led to the emerging theory of Network-Centric Warfare (NCW). The Naval Services instantiation of NCW is FORCEnet. "FORCEnet is the "glue" that binds together Sea Strike, Sea Shield, and Sea Basing. It is the operational construct and architectural framework for naval warfare in the Information Age, integrating warriors, sensors, command and control, platforms, and weapons into a networked, distributed combat force. FORCEnet will provide the architecture to increase substantially combat capabilities through aligned and integrated systems, functions, and missions.

Sea Power 21 is a comprehensive attempt to address the ramifications of the Information Age revolution. The framework of the Sea Power 21 vision is composed of the following elements: Sea Basing, Sea Shield and Sea Strike. The enabler of this vision or the "glue" that holds it all together is FORCEnet. FORCEnet is "the operational construct and architectural framework of naval warfare in the information age that integrates Warriors, sensors, networks, command and control, platforms, and weapons into a networked, distributed combat force that is scaleable across all levels of conflict from seabed to space and sea to land."

The Trident Warrior 03 exercise was then developed as a means to measure its success and to acquire data from which future exercises can be measured against. FORCEnet is still in its infancy and many people have different views on what exactly it is and how it should be implemented to achieve those goals. The intent of this thesis was not to answer those questions per se, but provide a realistic analysis of what worked during the TW03 exercise and what did not. This should provide a baseline for further Trident Warrior exercises so as to avoid the same mistakes in the future. The military has a ways to go before it can fully realize a truly networked-centric armed forces, but TW03 was the beginning and the lessons learned from it will pay dividends in realizing that fully networked goal.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

This Thesis would not have been possible without the loving support of my wife Maria and my two boys Johnny and Joey. Their unconditional love has been a driving force behind my work at NPS and I cannot say enough how grateful I am for their enduring patience and support.

I would also like to extend my thanks to Professors Dan Boger and Susan Higgins. Without their patience, support and guidance this Thesis would not have come to fruition.

Finally, to all my classmates who have endured the last two years of projects, homework and exams, I would like to say “Thank You” for making my stay at NPS a memorable one. Good luck and God speed to you and your families.

THIS PAGE INTENTIONALLY LEFT BLANK

EXECUTIVE SUMMARY

Since the country has moved into the Information Age, the military forces have been moving towards network based operations. The rapid expansion of the internet and information technology (IT) has led to the emerging theory of Network-Centric Warfare (NCW). The Naval Services instantiation of NCW is FORCEnet. "FORCEnet is the "glue" that binds together Sea Strike, Sea Shield, and Sea Basing. It is the operational construct and architectural framework for naval warfare in the Information Age, integrating warriors, sensors, command and control, platforms, and weapons into a networked, distributed combat force. FORCEnet will provide the architecture to increase substantially combat capabilities through aligned and integrated systems, functions, and missions.

Sea Power 21 is a comprehensive attempt to address the ramifications of the Information Age revolution. The framework of the Sea Power 21 vision is composed of the following elements: Sea Basing, Sea Shield and Sea Strike. The enabler of this vision or the "glue" that holds it all together is FORCEnet. FORCEnet is "the operational construct and architectural framework of naval warfare in the information age that integrates Warriors, sensors, networks, command and control, platforms, and weapons into a networked, distributed combat force that is scaleable across all levels of conflict from seabed to space and sea to land."

The Trident Warrior 03 exercise was then developed as a means to measure its success and to acquire data from which future exercises can be measured against. FORCEnet is still in its infancy and many people have different views on what exactly it is and how it should be implemented to achieve those goals. The intent of this thesis was not to answer those questions per se, but provide a realistic analysis of what worked during the TW03 exercise and what did not. This should provide a baseline for further Trident Warrior exercises so as to avoid the same mistakes in the future. The military has a ways to go before it can fully realize a truly networked-centric armed forces, but TW03 was the beginning and the lessons learned from it will pay dividends in realizing that fully networked goal.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. BACKGROUND

Since the country has moved into the Information Age, the military forces have been moving towards network based operations. The rapid expansion of the internet and information technology (IT) has led to the emerging theory of Network-Centric Warfare (NCW). The Naval Services instantiation of NCW is FORCEnet. "FORCEnet is the "glue" that binds together Sea Strike, Sea Shield, and Sea Basing. It is the operational construct and architectural framework for naval warfare in the Information Age, integrating warriors, sensors, command and control, platforms, and weapons into a networked, distributed combat force. FORCEnet will provide the architecture to increase substantially combat capabilities through aligned and integrated systems, functions, and missions. It will transform situational awareness (SA), accelerate speed of decision, and allow us to greatly distribute combat power."[1]

The Trident Warrior 03 (TW03) was a Fleet Command, Control, Communications, Computers, Information, Surveillance and Reconnaissance (C4ISR) experiment cosponsored by CNO, NETWARCOM, and SPAWAR to demonstrate FORCEnet capabilities with existing Navy C4ISR products. This was the first large scale Sea Trial event focused on "speed to capability" for initial FORCEnet delivery to a Joint operational environment, by exercising robust, dynamically reconfigurable networks to support integrated fires and command and control for the ESSEX Expeditionary Strike Group. The three main areas that the evaluation focused on were: Dynamic, multi-path, survivable networks, Distributed, collaborative command and control and Expeditionary, multi-tiered sensor and weapon information.

B. OBJECTIVE

The objective of this thesis is to show the reader how the evolution of technology and the Information age led to the concept of Network-Centric Warfare, from which FORCEnet evolved. Then as a means to measure the ability to implement such a concept, the Trident Warrior series of exercises was born. This thesis will give the reader

[1] Clark, Vern, Admiral, U.S. Navy, Chief of Naval Operations. Sea Power 21: Projecting Decisive Joint Capabilities, October 2002, p. 10.

an understanding of where the military has been and what direction it intends to move to in the 21st Century.

C. SCOPE AND METHODOLOGY

1. Scope

The thesis begins with an overview of military transformation in the Information Age and describes how the military is moving from its Platform Centric Doctrine exhibited in the Cold War era Industrial Age to the Network Centric Doctrine that is prevalent in the Information Age. The thesis will then describe the theory of Network-Centric Warfare which led to the Navy's instantiation of it called FORCEnet.

NCW theory was tested against Trident Warrior 03, an experiment to test the validity and ease of implementation of the FORCEnet concept.

2. Methodology

Because of the rapidly evolving nature of FORCEnet and Network-Centric Warfare, the majority of the research was performed through review of books, magazines, web sites and prior theses. The data that was collected for this thesis came from various program offices and resource sponsors, especially the data that was needed for the Trident Warrior 03 exercise. Interviews are used to fill in other areas to support the research findings.

3. Primary Research Question

a. How successful was TW03 in implementing NCW theory? If portions of the experiment were unsuccessful, what were the major causes?

b. What areas of the NCW theory were substantiated by the exercise?

c. Where were the gaps between theory and practice?

4. Subsidiary Research Questions

a. What is the conceptual framework for Network Centric Warfare and how does it relate to TW03?

b. What can the Military learn from TW03 that can be applied to future exercises to help substantiate NCW theory?

5. Benefits of the Study

The anticipated benefit from this study is to test that the Network Centric Warfare (NCW) theory tenets against Trident Warrior 03 exercise. These tenets state that: "1. A robustly networked force improves information sharing; 2. Information sharing and collaboration enhance the quality of information and shared situational awareness; 3. Shared situational awareness enables collaboration and self-synchronization and enhances sustainability and speed of command; and 4. These in turn dramatically increase mission effectiveness."[2]

The results from TW03 will help substantiate that NCW theory is the guiding path the military should take in its transformation process. Perhaps the biggest benefit of this thesis is to reaffirm that the Naval Services are following the Global trends of the information age and is moving towards a Networked Centric Force. However, there are certain areas that need specific attention. For example, two areas that the military is lagging behind in are the cognitive domain (conveyed commander's intent, planning, organizing, deploying cycle), and the social domain (the intersection of people living and working together). The military is strong in the physical domain (the tangible world of objects and actors) and the information domain (the figurative space where information resides and is transferred)[3] but until there is a synergy between all four domains the U.S. Armed Forces will never be fully realized into a flexible, adaptable Information Age force.

6. Organization of the Thesis

Chapter I is the background and organization of the thesis.

Chapter II is an introduction to military transformation in the Information age and what the military needs to do to stay competitive in this ever-changing global environment.

Chapter III is an introduction to Network-Centric Warfare and Sea Power 21.

---

[2] Garskta, John. An Introduction to Network Centric Operations. Presentation to NCO Short Course 13 July 2004.

[3] Holloman, Kimberly. Understanding the Network as a Verb. Presentation to NCO Short Course 13 July 2004.

Chapter IV focuses on the development of FORCEnet as the Naval Service's answer for a Network-Centric force.

Chapter V is an analysis of Trident Warrior 03 and an overall summary of the implementation of FORCEnet in experiment form.

Chapter VI discusses conclusions and possible areas for further research.

II. MILITARY TRANSFORMATION IN THE INFORMATION AGE

A. TRANSFORMATION IN THE DEPARTMENT OF DEFENSE

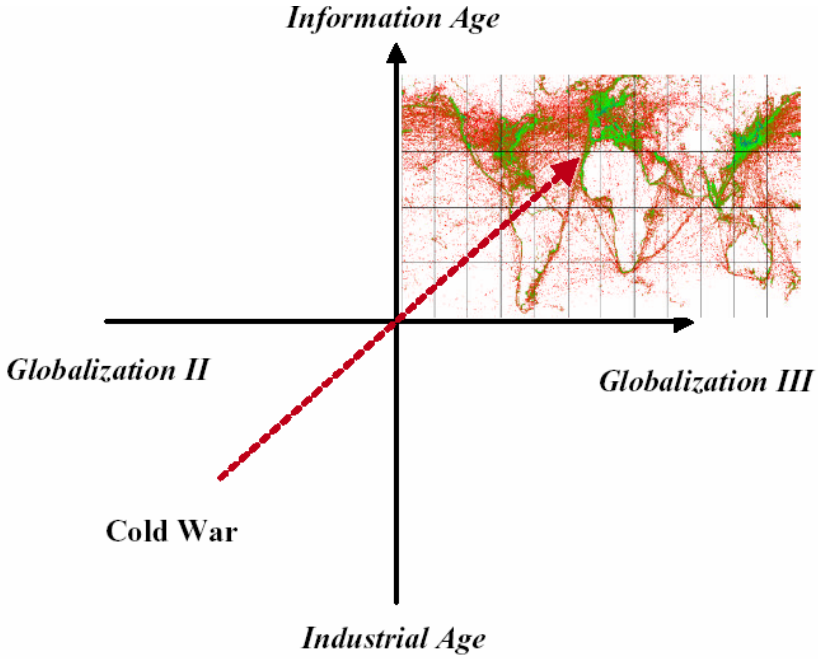
In today's Information Age the military must take advantage of the increasing presence of Information Technology and its role within the military. One of the Pentagon's top priority's is transforming the military into a leaner, faster, high tech warfighting machine. This transformation, known as the Revolution in Military Affairs (RMA), is vital for today's military to meet the ever changing threats that will occur in the 21st Century. Today's hostile powers find it very affordable to combat U.S. military dominance either by low-tech terrorism or high-tech cyberwarfare. Either way, this weakens the U.S. massive advantage in conventional forces. In his book, "Information Age Transformation", Dave Alberts states that "the DOD has moved from a threat-based strategy to a capabilities based strategy and the debate has shifted accordingly. The events of September 11th, 2001, have focused increasing attention on the need to transform the DoD's organization from one finely tuned for accomplishing traditional military missions to one that is capable of deterring, preventing, and if necessary, defeating a diverse set of nontraditional adversaries."[4]

However, today's military is still ensconced in Cold War-era relationships, hierarchies and planning based on the expectation of massive land warfare. This type of warfare was successful in the Cold War Industrial Age, but remaining competitive in the Information Age demands playing by a set of new rules. Success in the Information Age is dependent on adaptability, speed and agility. These traits were not valued in the Industrial Age. The forces that are the most maneuverable and that can get the right information at the right time that are going to be the most successful.

Figure 1 depicts the relationship between the two trends and the movement from the Industrial Age to the Information Age. The military is moving from the tenets of the Industrial age in the lower left quadrant of the graph to the global trends of the Information Age in the upper right quadrant of the graph.

[4] Alberts, David S. Information Age Transformation. June 2002. p.vii.

Figure 1. Transformation in the Information Age[5]



Information is power and is the world moves towards the upper right graph as presented in figure 1, Information Age concepts and technologies are being adopted by terrorists and asymmetrical adversaries who wage war against us; especially Information Warfare and Information Operations. The next section is an Information Warfare/Operations primer to give the reader an understanding of such concepts.

B. KEY CONCEPTS OF INFORMATION WARFARE

1. Key Definitions

Information Warfare has far reaching effects. As shown in Figure 2, Information Warfare includes not only the traditional military targets but political and civilian infrastructure as well. Command and Control Warfare (C2W) is the military application of Information Warfare. Command and Control Warfare is defined as "the integrated use of operations security (OPSEC), military deception, psychological operations (PSYOP), electronic warfare (EW) and physical destruction, mutually supported by intelligence, to

[5] Network Centric Operations: Understanding the Emerging Information Age Force. Conference at the Naval Postgraduate School, Monterey, California, July 12-15, 2004.

deny information to, influence, degrade or destroy adversary C2 capabilities, while protecting friendly C2 capabilities against such actions"[6]

To solidify the concepts of Information Warfare (IW) and Information Operations is important to define some concepts. These concepts will provide a better understanding of Network Centric Warfare and FORCEnet discussed later in this paper.

Information Operations (IO): Information operations involve actions taken to affect adversary information and information systems while defending one's own information and information systems. They apply across all phases of an operation, the range of military operations, and at every level of war. They are a critical factor in the joint force commander's (JFC's) capability to achieve and sustain the level of information superiority required for decisive joint operations. IO capitalizes on the growing sophistication, connectivity, and reliance on information technology. IO target information or information systems in order to affect the information-based process**,** whether human or automated. Such information dependent processes range from National Command Authorities-level decision making to the automated control of key commercial infrastructures such as telecommunications and electric power.[7]

Information Warfare (IW): Information warfare (IW) is IO conducted during time of crisis or conflict (including war) to achieve or promote specific objectives over a specific adversary or adversaries. Within the context of the joint force's mission, the joint force commander (JFC) should apply the term "adversary" broadly to include organizations, groups, or decision makers that may adversely affect the joint force accomplishing its mission.[8]

Information: 1. Facts, data, or instructions in any medium or form. 2. The meaning that a human assigns to data by means of the known conventions used in their representation[9].

---

[6] Joint Publication 3-13, Joint Doctrine for Information Operations, 09 October 1998, p. 3.

[7] Ibid, p. vii.

[8] Ibid. p.1-1.

[9] Joint Publication 3-13, Joint Doctrine for Information Operations, 09 October 1998.

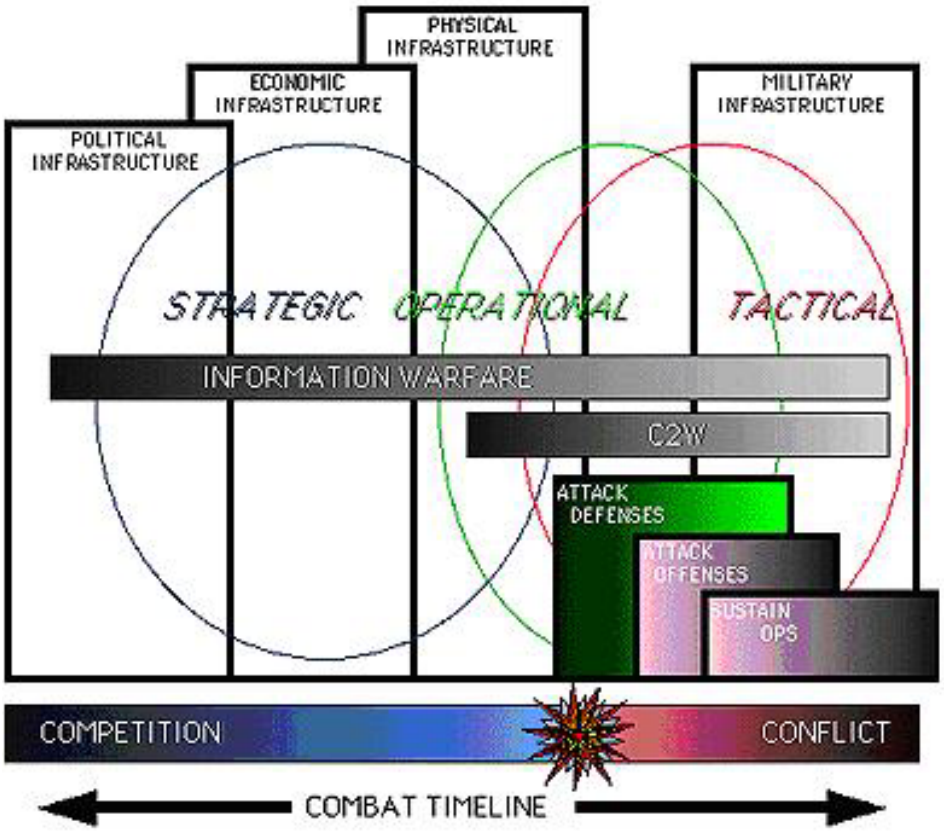


Figure 2. Information Warfare Architecture[10]

Information Superiority: The capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same.[11]

Intelligence: 1. The product resulting from the collection, processing, integration, analysis, evaluation, and interpretation of available information concerning foreign countries or areas. 2. Information and knowledge about an adversary obtained through observation, investigation, analysis, or understanding.[12]

---

[10] Ibid, p. 3-13.

[11] Ibid.

[12] Joint Publication 1-02Department of Defense Dictionary of Military and Associated Terms, 12 April 2001, p. 261.

The next section defines how information age principles and phenomena are changing the character of warfare and homeland security. Access to highly capable, low-cost IT technology is a global trend that is leveling the playing field and plays against the strengths of conventional warfare that was prevalent in the Industrial age.

C. THE VALUE OF IT ON INFORMATION OPERATIONS

1. The New Terrain

Information Technology (IT) has become so important in establishing dominance in the military arena that it almost overwhelms everything else. IT has become such a force multiplier that the right technologies, used intelligently, makes having superior numbers seem almost irrelevant. A turning point in understanding the value of IT was demonstrated in the first Gulf War in 1991. Iraq had the third largest army in the world and had just killed 300,000 Iranians in their eight years of warfare. American generals faced the same problem as the Iranians: How to dislodge Iraqi's that were well fortified in dug-in positions? Most feared that the United States and its coalition forces would suffer catastrophic casualties but when the war was over only 240 personnel had lost their lives. Comparatively speaking Iraq had suffered about 10,000 casualties. The difference was information technology. The Americans and their allies could see at night, drive through a featureless desert with the aid of a Global Positioning System (GPS) and use smart bombs to destroy targets with a 90 percent probability.[13]

One of the most interesting aspects of information technology on warfare is that the concept of "the front" has become obsolete and now information technology has become the difference between winning and losing.[14] Everyone and everywhere are part of the battlefield today. With the increasing coverage of satellites to aid the view of the battle space, combatants are finding it hard to avoid the reach of precision guided munitions.

Operational Iraqi Freedom (OIF) has buttressed the importance of information superiority. The Internet as a capability to rapidly share time sensitive knowledge and information is becoming the norm rather than the exception. Naval Officers are

[13] Berkowitz, Bruce The New Face of War: How War Will Be Fought in the 21st Century. The Free Press 2003, p. 3.

[14] Ibid., p. 4.

becoming well versed in monitoring multiple chat rooms to dissect and analyze critical intelligence. However, according to Captain John Mackercher, USN, we still have a ways to go.

> Although employment of information technologies was successful in the main, there are specific areas where improvements must be made. For example, standardized protocols should be developed to ensure consistent understanding and proper usage. Log-keeping requirements for chat also lack adequate definition. In our experience, mIRC, a recently adopted software upgrade, is a much more capable program than MS Chat. The former has the ability to time stamp transmissions and includes an autolog capability. The Navy should study the inclusion of mIRC with IT-21 installations.[15]

As Captain Mackercher's statement applies, the Naval Forces are making great strides with the advancement of information technology and utilizing it to improve their efforts in gaining information superiority. But, as he states, there is room for improvement and if the U.S. is going to remain steadfast in its transformation in the information age, it needs to continue to develop and exploit existing technologies to its fullest extent, and above all, continue to train and develop our service men and women in these new technologies.

Every war teaches the world something about the ever-changing nature of warfare and Operation Iraqi Freedom (OIF) was no different. "The distinctive feature of this war is rapidity: of battlefield intelligence, of fire, of change in tactics, of large unit movement, of reporting and of national mood."[16] Our real time battlefield intelligence permits tip-of-the spear reconnaissance that permits units to avoid enemy mass engagements. The quickened pace of battlefield communications enables what General Tommy Franks

---

[15] Mackercher, John We have More to learn form Iraqi Freedon, Proceedings. August 2004. p. 76.

[16] Battle Speed. Washington Times. April 7, 2003.

refers to as “the flexibility of the strategic plan”. The capacity for mid-battle redeployment of large and small units is accredited to decentralized command and pushing the commander’s intent to the lowest level decision makers so that this information sharing and collaboration leads to a more maneuverable force. This is one of the major tenets of NCW.

The next chapter deals with the origin and future of NCW. It begins with Joint Vision 2020 and goes through the conceptual framework of NCW. These concepts are the underpinnings of FORCEnet which TW03 is measured against.

THIS PAGE INTENTIONALLY LEFT BLANK

III. NETWORK CENTRIC WARFARE

Chapter II provided the background for and the rationale behind the evolution of Network Centric Warfare (NCW), which is the foundation of FORCEnet. Joint Vision 2020 supplies the building blocks of the NCW theory and it is summarized in section A.

A. JOINT VISION 2020

Joint Vision 2020 builds upon the architecture that was established in Joint Vision 2010 which was a guide for the transformation of America's armed services. "The overall goal of Joint Vision 2020 is the creation of a force that is dominant across the full spectrum of military operations-- persuasive in peace, decisive in war, preeminent in any form of conflict."[17]

1. Operational Concepts

The operational concepts of Joint Vision 2020 remain the same as they did with Joint Vision 2010. Dominant maneuver, focused logistics, precision engagement and full dimensional protection are the key operational concepts that remain the same. The focus of Joint Vision 2020 is to develop a strategic approach to prepare our forces for an uncertain future. The operational concepts are defined as follows:

- Dominant Maneuver

Dominant maneuver is the ability of joint forces to gain positional advantage with decisive speed and overwhelming operational tempo in the achievement of assigned military tasks. Widely dispersed joint air, land, sea amphibious, special operations and space forces capable of scaling and massing force or forces and the effects of fires as required for either combat or noncombat operations, will secure advantage across the range of military operations through the application of information, deception, engagement, mobility and counter-mobility operations.[18]

- Focused logistics

Focused logistics is the ability to provide the joint force the right personnel, equipment and supplies in the right place, at the right time, and in the right quantity, across the full range of military operations. This will be made possible through real time,

[17] Joint Vision 2020: America's Military Preparing for Tomorrow

[18] Ibid. p. 20.

web-based information system providing total asset visibility as part of a common relevant operational picture, effectively linking the operator and logistician across Services and support agencies. Through transformational innovations to organizations and processes, focused logistics will provide the joint warfighter with support for all functions.[19]

- Precision Engagement

Precision engagement is the ability of joint forces to locate, survey, discern and track objectives or targets; select, organize, and use the correct systems; generate desired effects; assess results; and reengage with decisive speed and overwhelming operational tempo as required throughout the full range of military operations.[20]

- Full Dimensional Protection

Full dimensional protection is the ability of the joint force to protect its personnel and other assets required to decisively execute assigned tasks. Full dimensional protection is achieved through the tailored selection and application of multilayered active and passive measures, within the domains of air, land, sea, space, and information across the range of military operations with an acceptable level of risk.[21]

2. What's Changed Since JV 2010?

The goal still remains focused on operational forces and the main objective is to be decisive in war and to expand to address the full range of operations. But there have been some changes and a shifting of focus in three areas: strategic context, full spectrum dominance and information superiority.

a. Strategic Context

Strategic context has been narrowed down to three main aspects: global interests, diffused technology and adaptive enemies. "The joint force of 2020 must be prepared to "win" across the full range of military operations in any part of the world, to operate with multinational forces and to coordinate military operations, as necessary, with government agencies and international organizations".[22] This is clearly evident with the type of operations that are currently being conducted in Operation Iraqi Freedom

[19] Ibid., p. 24.

[20] Ibid., p. 22

[21] Ibid., p. 26

[22] Ibid., p. 4

(OIF). The United States has not only had to rely on its coalition partners for support but also move into the unfamiliar territory of a security force to help establish a democratic government.

With diffused technology it is not always possible to attain a wide margin of a technological advantage over all our adversaries due to the increasing availability of commercial off the shelf (COTS) technologies. Virtually nine-tenths of our military communications travel over commercial links.[23] Add that the Pentagon buys most of its hardware and software off the shelf and our adversaries have the opportunity to exploit the same technology that is available to the U.S. However, our advantage must be obtained by our leaders being superiorly trained in the latest technologies so that we can exploit existing shared technologies to our advantage and put our adversaries on the defensive.

Adaptive enemies increasingly rely on "asymmetric threats"- strategies and tactics that avoid our strengths head on and instead hit us where we are weak.[24] There is no better example of an asymmetric attack than that of 9/11. By using computers, satellite communications, and the Internet, Al Qaeda pre-deployed its strike forces in America and Canada. Bin Laden controlled these forces from halfway around the world using a communication network of cells, which in turn coordinated its actions within this decentralized network. To defeat these adaptive enemies the U.S. must first be able to win the information war by making our own information systems more capable, reliable and secure, or by attacking our adversary's information systems leaving them vulnerable and less secure.

b. Full Spectrum Dominance

The ultimate goal of our military is to win wars and achieve the objectives directed by the National Command Authorities. Joint forces of the future will accomplish these goals by achieving full spectrum dominance- the ability of US forces, operating unilaterally or in combination with multinational and interagency partners, to defeat any adversary and control any situation across the full range of military operations.[25]

---

[23] Berkowitz, p. 138.

[24] Ibid.,.7

[25] JV 2020, p. 6.

To achieve full spectrum dominance the US forces will need to operate in all domains- space, sea, land, air and information and do so unilaterally with a combination of forces tailored to specific situations. To meet these challenges will require a total force composed of well-educated, motivated, and competent people who can adapt to the many demands of future joint missions. The transformation to a joint force to reach full spectrum dominance is incumbent upon information superiority as a key enabler and our capacity for innovation.[26] (see Figure 3 below)

Figure 3. Full Spectrum Dominance[27]

[26] Ibid., p. 7.

[27] Ibid, p.7.

c. Information Superiority

In future warfare, the struggle for information will play a central role, taking the place, perhaps, of the struggle for geographical position held in previous conflicts. Information superiority is emerging as a newly recognized, and more intense, area of competition.[28] Information Superiority is defined as:

The capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same.[29]

Information processing and a military leader's ability to assess and disseminate information quickly and efficiently has been the key enabler of victory on the battlefield.

Information Superiority provides a commander with a competitive advantage when it is translated into knowledge that can make superior decisions. The Joint force must be able to take advantage of this superior knowledge to achieve "decision superiority"-better decisions arrived at and implemented faster than an opponent can react, or in a noncombat situation, at a tempo that allows the force to shape the situation or react to changes and accomplish its mission.[30]

The evolution of technology and communications systems has allowed for the integration of information operations and intelligence, surveillance, and reconnaissance (ISR) in a fully integrated campaign. The concept of the Global Information Grid (GIG) is the main enabler of network-centric environment.[31] "The Global Information Grid is the globally interconnected, end-to-end set of information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel."[32]

---

[28] Arquilla, John and Ronfeldt, David. In Athena's Camp: Preparing for Conflict in the Information Age, Rand Publications, 1997, p. 90.

[29] Joint Publication 3-13, Joint Doctrine for Information Operations, 09 October 1998. p. I-10.

[30] Joint Vision 2020: America's Military Preparing for Tommow, p..8.

[31] Ibid., p. 9.

[32] Department Information Systems Agency Website, www.disa.mil/main/prodsol/gig_be.html, visited 15 July 2004.

With the building blocks of NCW laid, the next section focuses on the Military's implementation of technology to move away from a platform-centric force to one that evolves around the "network".

B. NETWORK CENTRIC WARFARE

> U.S. forces must leverage information technology and innovative network-centric concepts of operations to develop increasingly capable joint forces. New information and communications technologies hold promise for networking highly distributed joint and multinational forces...
>
> Secretary of Defense Donald Rumsfeld

1. An Introduction to NCW

As was just discussed, Joint Vision 2020 provided the building blocks of Network Centric Warfare, which are the roots of the FORCEnet concept. In their book *Network Centric Warfare,* Alberts, Garstka, and Stein define Network Centric Warfare (NCW) as follows:

> An information superiority-enabled concept of operations that generates increased combat power by networking sensors, decision makers, and shooters to achieve shared awareness, increased speed of command, higher tempo of operations, greater lethality, increased survivability, and a degree of self synchronization.[33]

In essence, NCW translates information superiority into combat power by effectively linking knowledgeable entities in the battlespace. The three pillars of NCW are:

- Self Synchronization – The ability of a well- informed force to organize and synchronize complex warfare activities from the bottom up. The organizing principles are unity of effort, clearly articulated commander's intent, and carefully crafted rules of engagement. Self-synchronization is enabled by a high level of knowledge of one's own forces, enemy forces, and all appropriate elements of the operating environment. It overcomes the loss of combat power inherent in top-down command directed synchronization characteristic of more conventional doctrine and converts combat from a step function to a high-speed continuum.[34]

---

[33] Alberts, David S., et al. *Network Centric Warfare*, 5th edition. CCRP, October 2003. p. 2.

[34] Hesser, Woodrow and Rieken, Danny. *FORCEnet Engagement Packs: "Operationalizing" FORCEnet to Deliver Tomorrow's Naval Network-Centric Combat Reach Capabilities...Today.* December 2003. p. 43.

- Remote Sensor Engagements – Historically, DoD has focused on platform-centric operations, whereby combat power is often sub-optimized due to the fact platforms are unable to generate engagement quality information at ranges greater than or equal to the maximum engagement range of the platform's organic weapons. In contrast, network-centric operations focus on engagements facilitated via robust networks and digital data links that will allow the optimized use of weapons and sensors independent of platform restrictions.[35]

- Shared Battlespace Awareness - This concept is often mistakenly considered as a single picture or a perspective that must be common amongst all users or participants. Actually, NCW holds that battlespace awareness really exists in a distributed form. From the user's perspective, only a slice of "operational picture" is available at any given time. This view can take the form of either a particular detail or a more general, overall perspective. The ability to move up and down these levels of abstraction without introducing distortions is a critical aspect of such an operational picture.[36]

Figure 4 depicts the Military as a Network-Centric Enterprise, via a diagram that graphically depicts the definition of NCW and the principles discussed above. Referring back to figure 1 in chapter II, these NCW principles clarify the characteristics that resemble the movement to the upper right quadrant in the Information Age.

NCW broadly describes the combination of tactics, techniques and procedures that a networked force can employ to create a decisive warfighting advantage. In the age of Information Warfare, NCW is an information superiority enabled concept of operations that is the framework of how the U.S. will train and fight in the information age.

> NCW generates increased combat power by networking sensors, decision makers, and shooters to achieve shared awareness, increased speed of command, high tempo of operations, greater lethality, increased survivability and degree of self-synchronization.[37]

---

[35] Ibid., p. 44.

[36] Ibid.

[37] NCW Primer CD-ROM. Network Centric Operations: Understanding the Emerging Information Age Force. Conference at the Naval Postgraduate School, Monterey, California, July 12-15, 2004. p. 3.

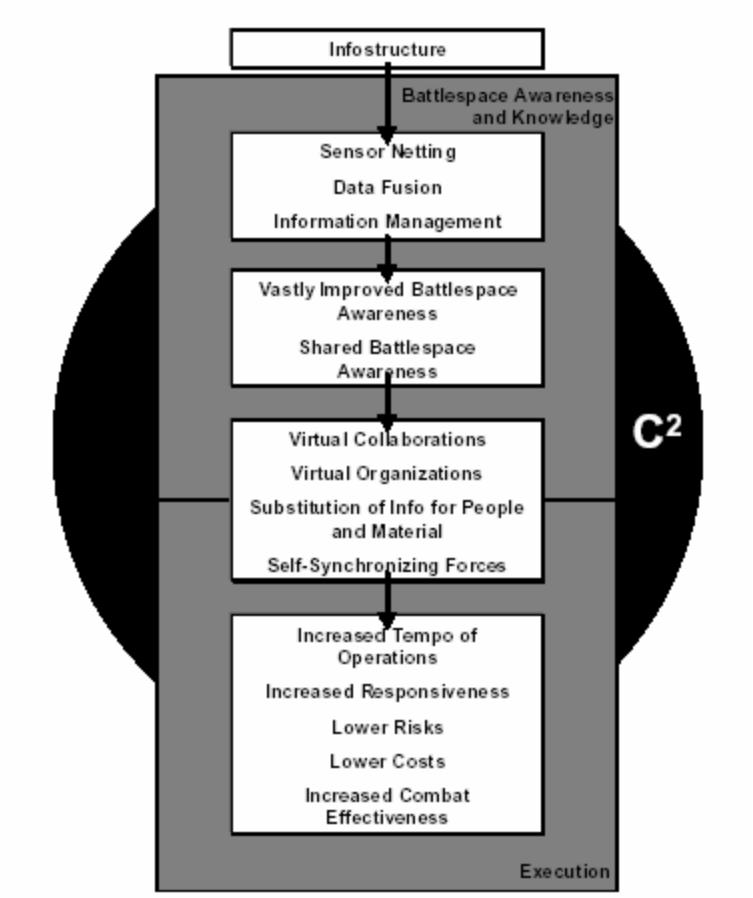


Figure 4. The Military as a Network-Centric Enterprise[38]

As a new source of power, NCW has a profound impact on the planning and conduct of war by allowing U.S. forces to get inside an adversary's decision cycle, changing the rules of warfare, and dictating the pace of military operations. NCW provides an edge at all three levels of military operations:

- **Strategy:** Selects a competitive space and determines the scope, pace, and intensity of the competition.
- **Operations:** Determines the key competitive attributes and applies / masters them.
- **Tactics:** Executed in the battlespace.[39]

The next section provides additional foundational concepts from which NCW theory was developed. One advantage that a networked-centric force provides over an

[38] Alberts, p. 89.

[39] NCW Primer, p. 3.

industrial age force is the speed of the decision making process. One of the major tenets of maneuver warfare is to have a faster decision cycle that your adversary. Air Force Colonel John Boyd transformed his energy maneuverability model into a decision making cycle that is taught throughout the military.

2. Decision Action Cycle- Boyd's OODA Loop

Air Force Fighter pilot John Boyd discovered in North Korea, in the 1950's, that the superior U.S. planes were consistently being shot down by the older more archaic Russian made planes, the MiGs. What Boyd realized that superiority in air combat had nothing to do with absolute speed, which is what the U.S.'s F-105s possessed, but what was more advantageous in combat was "transient" speed. That is, the ability to change directions much faster than your enemy, which is the ability that the Russian MiG-15s and MiG-17s possessed. Boyd originally coined this concept the "energy maneuverability model"[40]. He came to the conclusion that as American and Soviet aircraft came head to head in combat, the ability to move and countermove favored the Soviets. Boyd realized that the Soviets had better transient speeds which would give MiG pilots the advantage in a dogfight.

Boyd eventually reduced his model down to the acronym that recognizes the four steps required for outmaneuvering and dictating the flow of battle to your enemy: OODA (observation, orientation, decision, and action). "Gather data about your situation. Evaluate the data against your existing knowledge and your objective. Choose a course of action. Execute."[41] (See Figure 5 below)

[40] Berkowitz, p. 40.

[41] Ibid., p. 42.

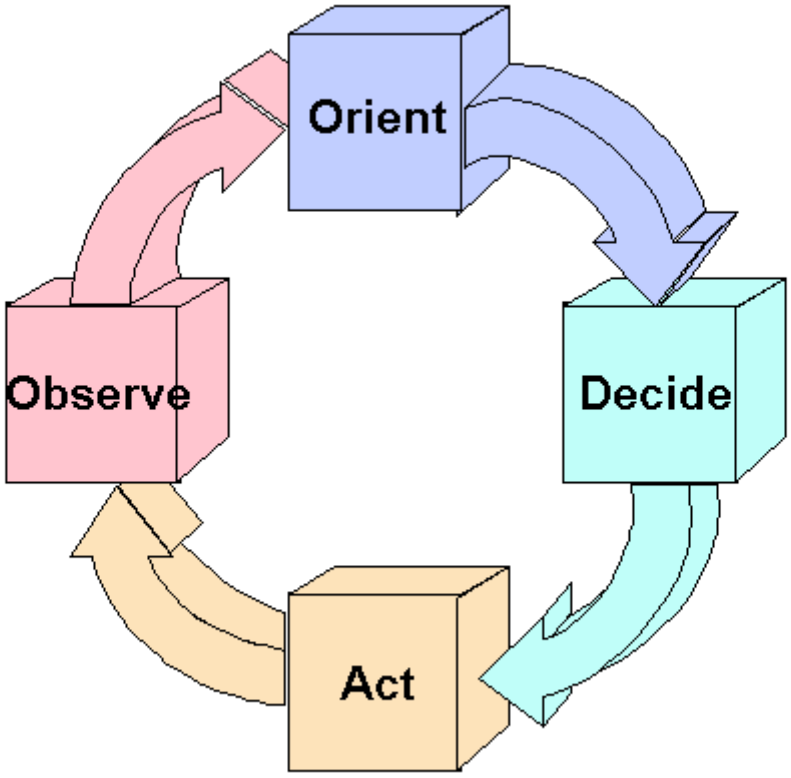


Figure 5. OODA Loop

Boyd went on to use his model on a larger scale and applied this theory to historical situations. "In the early stages of WWII, the French had a large well equipped standing army. In spite of this, the French army quickly dissolved in the face of the fast paced German blitzkrieg. The French were not defeated because they were outfought on an individual level, but because the Germans were operating at a pace the French were totally unprepared to match"[42]. What Boyd realized was that the OODA loop depended on collecting, processing, or moving information faster than one's opponent. By using this methodology, one can maintain a competitive advantage by forcing their enemy back on their heels and dictating the operational tempo (OPTEMPO).

This methodology is at the core of NCW. The goal of NCW is to network the forces so that the commander's intent and the updated intelligence can be shared throughout the battlespace. With the rapidity of information exchange between units, this

[42] Adkins, Mark and Kruse, John. Network Centric Warfare in the U.S. Navy Fifth Fleet. August 3, 2003. p. 6.

allows for a faster decision making cycle, thus creating a faster OODA loop that the adversary needs to react to. This gaining of information superiority is another of the Information Age tenets that is located in the upper right hand quadrant in figure 1.

With the definition of NCW stated and a brief history of its origins, the following section discusses the conceptual framework (CF) of NCW and the four dimensions which comprises its theory.

3. Conceptual Framework of NCW

A framework had been developed that can now be used. This framework will provide an architecture that could be used for making predictions about the application of technology and combat power. "The NCW Conceptual Framework (CF) is an effort at bringing all of the varied hypotheses together in one model"[43]. Figure 6 is the summary of the CF. This section will further clarify the CF framework.

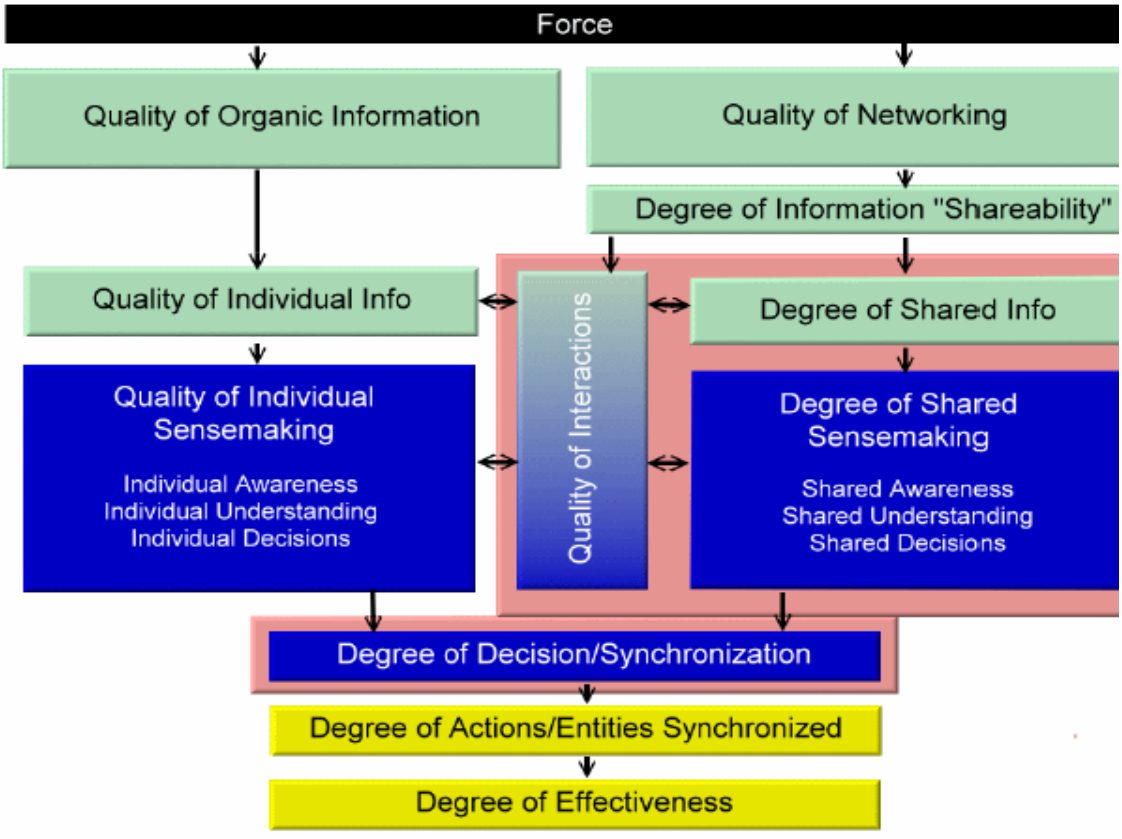


Figure 6. NCW Conceptual Framework

[43] Adkins, p. 8.

The CF is comprised of four dimensions:

1. The physical domain- the tangible world of objects and actors;
2. the information domain- the figurative space where information resides and is transferred;
3. the cognitive domain- the seat of individual and group thought, sensemaking and awareness; and
4. the social domain- the intersection of people living and working together, either in person or through the network.[44]

The following figure depicts a graphical representation of the four domains and how they interact with one another.

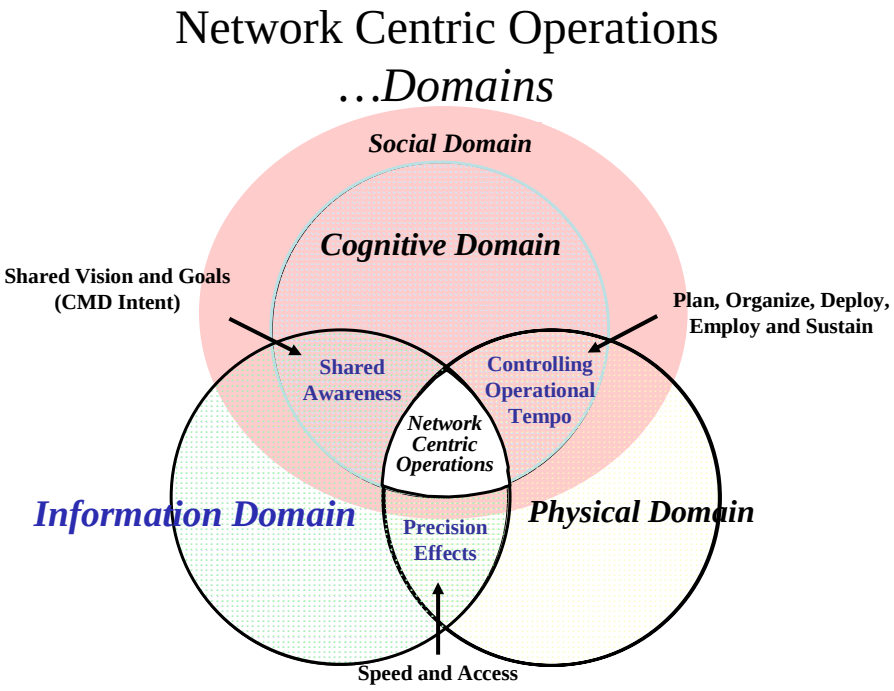


Figure 7. NCW Domains[45]

[44] Ibid., p. 9

[45] Holloman, Kim. Evidence Based Research Brief given at the NCO course at the Naval Postgraduate School, 15-18 July 2004.

> Briefly, the CF posits that an individual (or group) needs accurate and timely information to build situation awareness and understanding in the cognitive domain. The network allows the participants to both push and pull information from the information domain. By doing so, the aggregation of synchronized actors creates a virtual team in the social domain that works together toward common ends. Ultimately, the shared understanding allows warfighters to make effective decisions in line with the plans and goals of the group that can be enacted in the physical domain. Effectively, the team members working in parallel are able to accomplish far more through enlightened self-organization than would be possible through traditional hierarchical organization.46

Within the CF individuals are allowed to act independently, but always within realm of the commander's intent. The network allows the utilization of smaller more responsive flexible units. Instead of sending a self-supporting armor brigade, the commander may send in a Special Forces unit that has a smaller footprint but can use the network to gain greater firepower through coordinated supporting arms. Information superiority will eliminate command and control bottlenecks, be more efficient and effective. The following diagrams are a graphical walk through of NCW tenets which develop and codify the underlying theory of Network Centric Operations (NCO) through development, application and refinement of the NCO Conceptual Framework.

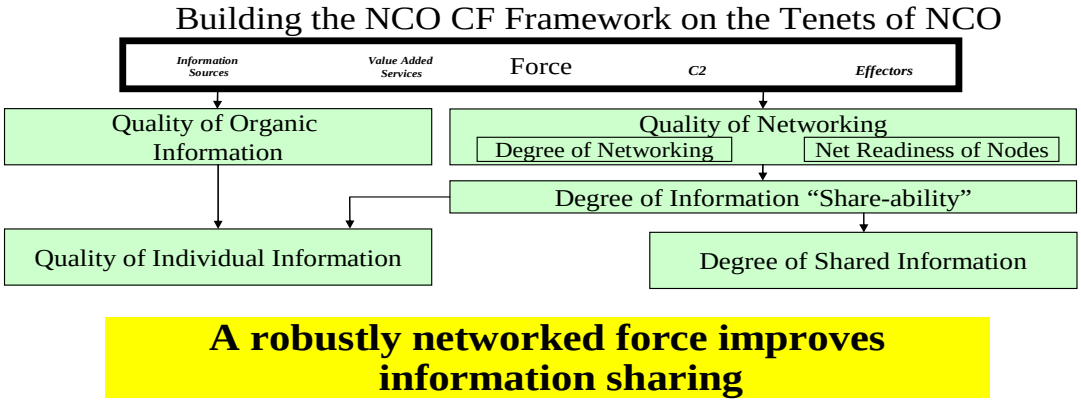


Figure 8. NCO Framework[47]

[46] Adkins, p.9

[47] Holloman, Kim. Evidence Based Research Brief given at the NCO course at the Naval Post Graduate School, 15-18 July 2004.

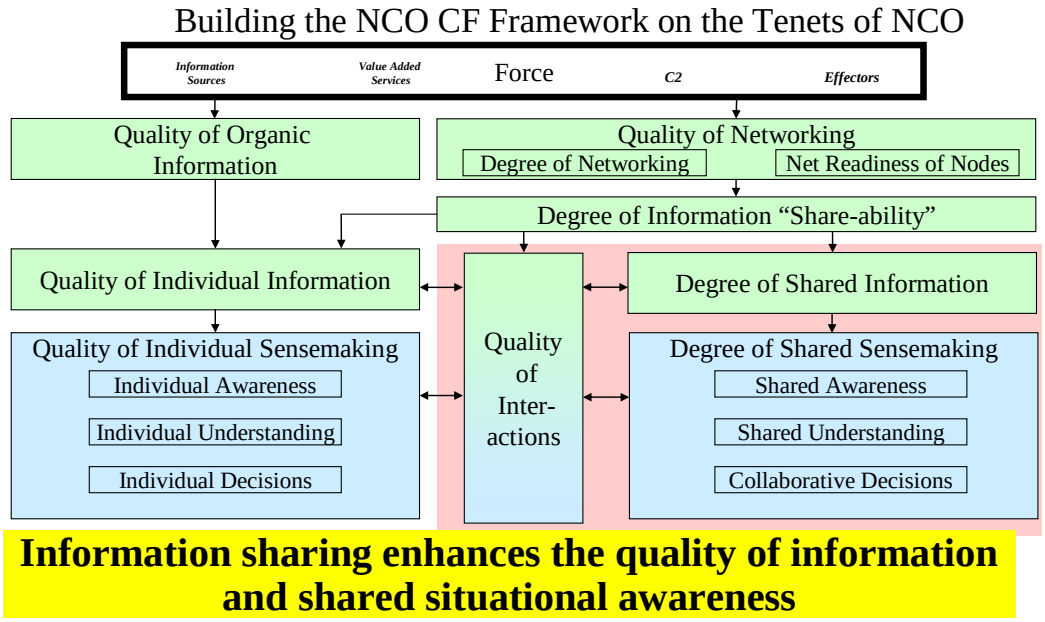


Figure 9. Information Sharing[48]

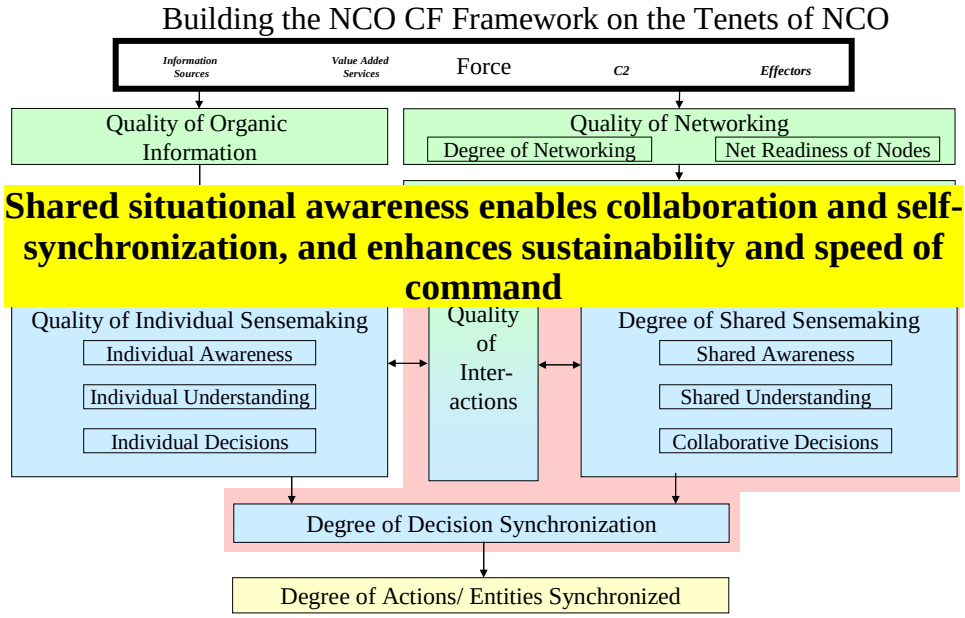


Figure 10. Shared Situational Awareness[49]

[48] Ibid

[49] Ibid

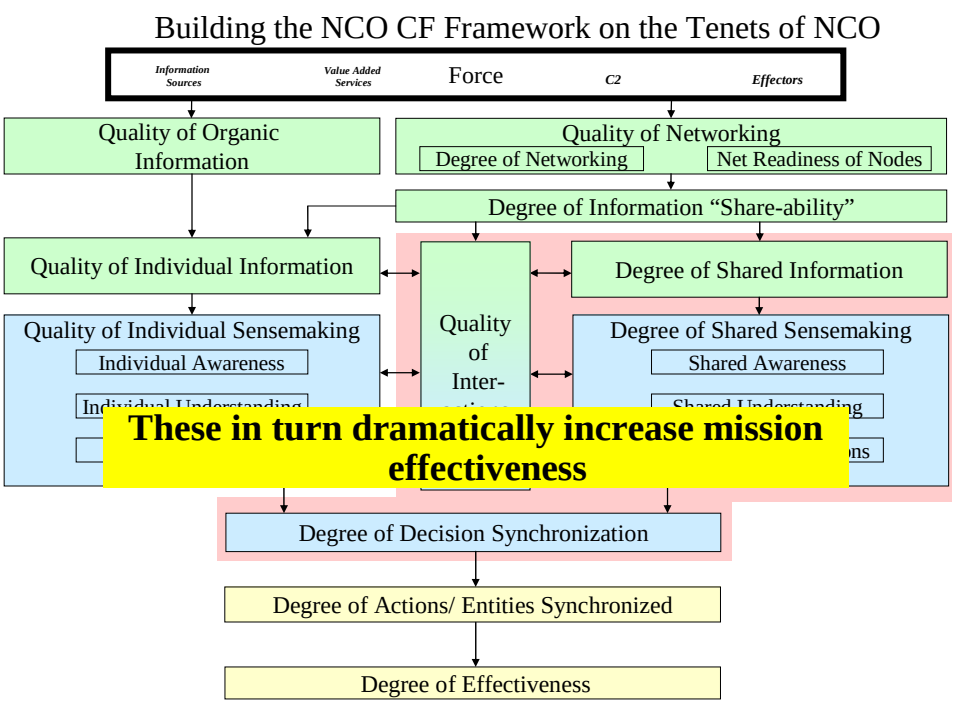


Figure 11. Increase in Mission Effectiveness[50]

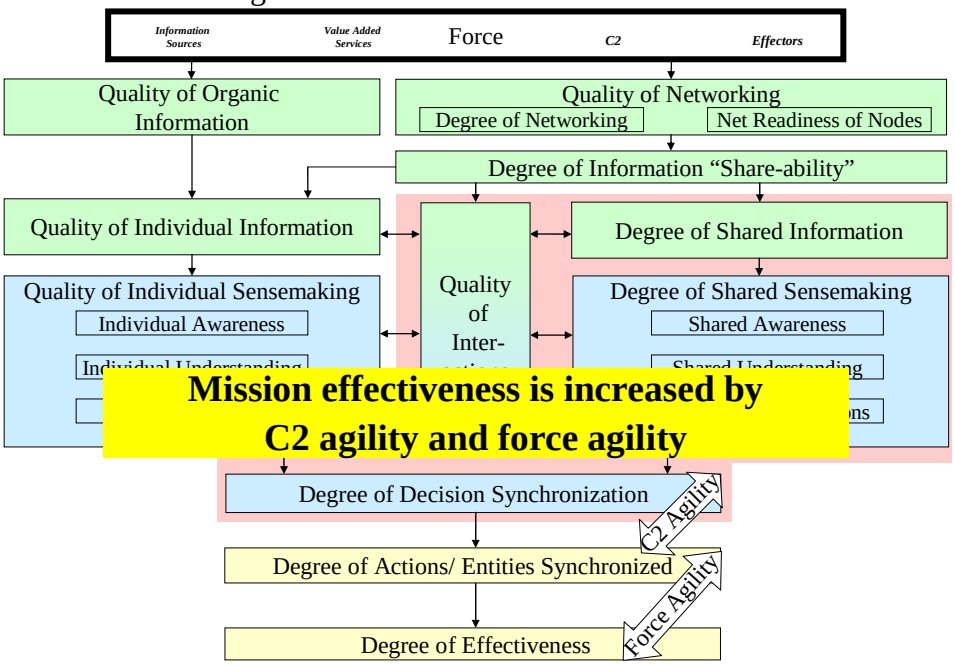


Figure 12. Increased C2 & Force Agility[51]

[50] Ibid

[51] Ibid

Technologies are evolving and emerging at a rapid rate in support of NCW tenets. These technologies are helping to crystallize the changing nature of warfare and help speed the progress to the upper right hand quadrant of the Information Age as shown in figure 1.

4. NCW Technologies

In the U.S. Fifth Fleet's Commander Task Force Fifty (CTF-50) case study, the key collaborative tools that were used in employment of NCW were Chat rooms, Knowledge Web (Kweb) and CommandNet.

a. Chat Rooms

Chat is a relatively ubiquitous technology that was primarily used in the civilian world for social interaction. Generally, the way chat works is that different channels or virtual rooms are set up on a server. These rooms are typically arranged to support a specific interest group. Within naval commands, the researchers have observed rooms centered on such interest groups as meteorology and oceanography (METOC), tomahawk land attack missile (TLAM) targeting, and logistics.[52]

b. Knowledge Web

The Knowledge web (Kweb) is a web-based information system originally developed by Space and Naval Warfare Systems Center. Command Carrier Group Three's first use of the Kweb capability was at the Global 2000 wargame. The concept was to display copious amounts of information to various members of the staff. The following is an excerpt from the exercise:

> The knowledge wall features a series of windows incorporating decision support tools tailored to the Commander Joint Task Force (CJTF), as well as windows with "summary status" information being "pushed" from the anchor desks used by liaison officers representing the various CJTF departments. The battlewatch captain in charge of the command center can choose which aspects of the situation to focus on by moving relevant content to the center of the wall and drilling down into deeper levels or related information. The knowledge desk uses software tools (COTS and information push Web applications) together with computer display hardware to enable the operator to create and publish value-added information to the Web. It consists of an integrated "desktop" spread across four different display surfaces. The top-right display is dedicated to routine office tasks such as preparing briefs, processing e- mail, writing

[52] Adkins., p. 15.

memos, etc. The top-center display is dedicated to providing the tactical situation “big picture” tailored to the user's decision-making needs. The bottom center display is a dedicated place for monitoring the execution of an operational plan. The top- left display is a tool explicitly designed to facilitate sharing information. The concept uses templates to “push” information from the operator to a Web site viewable by the rest of the command staff. The information “pushed” consists of worksheets, forms, and prompts to others on the command staff that would facilitate their understanding information relevant to their decision- making tasks. The software tools cause the information pushed to be formatted in a manner that others would recognize and understand, and published to a shared database in the Web environment.

The knowledge-wall hardware consists of a dual-processor Information Technology for the 21st Century (IT-21)-compliant workstation using three 4-port Appian Jeronimo Pro COTS video boards. The knowledge wall display is made up of ten 21-inch CRTs and two SmartBoard rear projection large-screen displays with internal liquid-crystal display (LCD) projectors. The displays operate as a single, integrated digital desktop, where each physical display has a resolution of 1024 by 768 pixels. This creates a digital desktop of 6144 by 1536 pixels. An additional CRT was dedicated to video and video teleconferencing requirements. The peripheral displays were intended to provide summary information for each of 14 functional areas of the CJTF command identified through knowledge engineering with the staffs of the U.S. Navy Third Fleet, Carrier Group One, and Carrier Group Three. Each summary display is formatted consistently by using a template-authoring tool that facilitates the creation of, and linking to, a variety of Web content without the operator responsible for producing content having to know hypertext mark-up language (HTML). Additional authoring tools were provided to facilitate the creation and publishing of map-based tactical data. All pages are implemented as HTML pages on a common server, with numerous links to more detailed pages for supplemental information. The title line indicates the functional areas described by the display. The “stop lights” in the top-left quadrant are intended to be viewable from 15 to 20 feet away, and indicate the status of activities in various time frames. Light colors indicate the severity of the alerts in terms of their deviation from the plan. The bottom- left quadrant provides space for a summary graphic or multimedia object. The right side of the screen provides space for amplifying links/headlines. The “Alerts” section describes specific problems within this domain/ functional area that might be of interest to others. The “Impacts” links describe the impacts of alerts in terms of effects on other functional areas. The “Links” area allows access to reference and supplemental material. Any text or graphic in the page may be linked to a more detailed Web page.[53]

[53] Ibid., pp. 15-16.

c. Command Net

The Defense Advanced Projects Agency (DARPA) sponsored the Center for the Management of Information's (CMI's) initial development of CommandNet in 1996 with a one-year research grant. The original DARPA research directive was both broad and flexible. CMI was required to share collaborative technology expertise with the staff of the U.S. Navy's Third Fleet and the component Commands while learning about collaborative processes within the U.S. Navy. The development of the initial CommandNet prototype came after a year of researchers being underway observing, interacting, and effectively becoming members of the Third Fleet staff. During the course of this research the CMI team members spent months on board all types of U.S. Navy ships studying the requirements of battle staffs and commanders. Command Net developed from a need for group situation awareness within the intelligence community of the Third Fleet staff.[54]

The CTF-50 case study is of significant value in the investigation of NCW theory and that it is the first study of a staff at the operational level of war, specifically the case of naval warfare. The following section details the benefits of NCW versus platform centric warfare.

5. Benefits of NCW

The real value of a networked force is that joint forces that can integrate NCW capabilities and are able to exploit the dependent nature of information warfare. They do so by altering the initial conditions, developing and sustaining high rates of change and keep the enemy ensconced in the fog of war. In doing so, this increases "battle speed"-speed of deployment, speed of organization, speed of employment, and speed of containment. Networking is the key that gives the U.S. and its coalition partners the ability to decide and act faster than our enemies. Figure 13 gives a graphical depiction of how a networked force moves the graph to the left, which is an indicator of increased speed. Also note that the intensity level is less than what a traditional platform-centric force creates. This is due to the fact that a network force can collect and process information faster and can avoid large scale mass on mass engagements.

[54] Ibid., p.16.

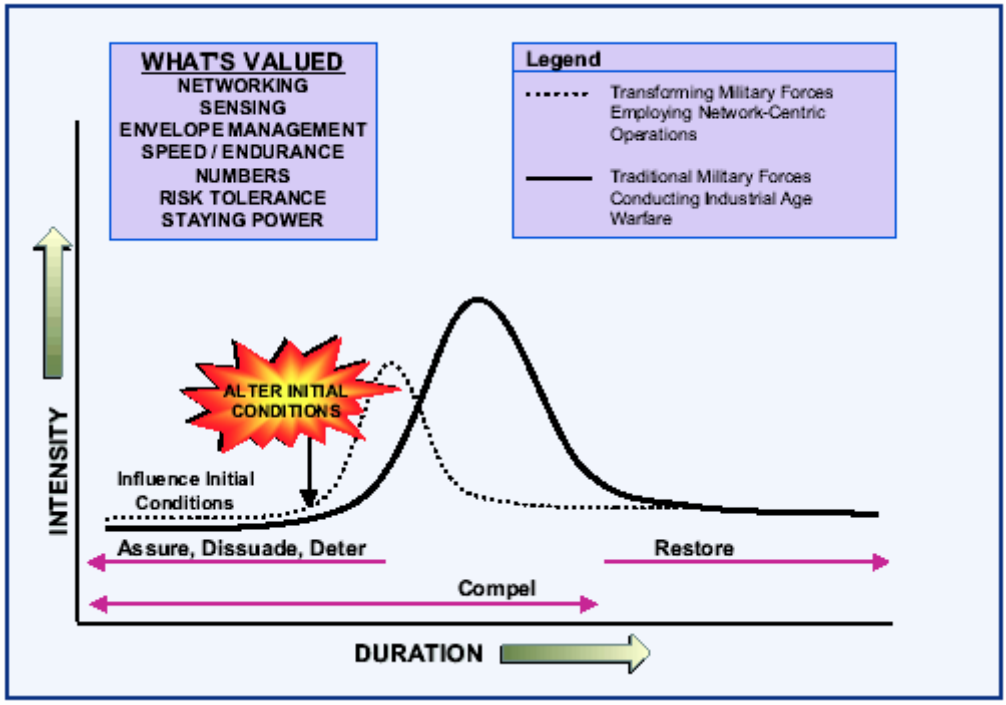


Figure 13. Networking vs. Platform Centric Forces[55]

As we begin the new millennium the U.S. is facing a new type of warfare. This revolution in military affairs (RMA) is recognized by the fact that any entity today can wage war, and increasingly the tools of war are increasingly marketplace commodities. Network Centric Warfare is the new model, and it represents a new way of thinking and engaging this modern enemy. The main component to this model is based on the premise that information must be exchanged more efficiently and effectively. This new thinking is having a radical effect on the planning and pacing of war. Traditionally commanders would launch a bombing mission only after hours of meticulous planning. But, "In Enduring Freedom 75 percent of the time aircraft did not even know what their targets were before they took off. Special Forces on the ground would locate targets and pass the GPS coordinates to B-52 bombers orbiting overhead. In other words, Just In Time military operations."[56] The next chapter describes the Naval Services instantiation of NCW; FORCEnet and how the Naval services plan to implement NCW into a viable military force structure.

[55] Ibid.

[56] Berkowitz, p. 114.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. FORCENET: ENABLING THE INFORMATION AGE WARRIOR

> FORCEnet is the centerpiece of our roadmap to the future. Once implemented, FORCEnet will effectively give warfighters the knowledge of the battlefield to 'know first' and 'act first'- taking advantage of knowledge superiority over an adversary to prevail in battle.
>
> Admiral Vern Clark, Chief of Naval Operations

FORCEnet is still in its infancy and its scope and implications are not yet fully realized throughout the U.S. Military. Although FORCEnet is a concept whose time has come and is being put into practice through military exercises, there are still many personnel who are quite skeptical of it as doctrine. Organizational change is a very difficult process and moving away from a platform centric military with cold war era technology to a network centric philosophy such as FORCEnet is proving to be a very difficult task.

A. FORCENET READINESS

The Director of FORCEnet is the Deputy Chief of Naval Operations for Warfare Requirements and Programs (CNO N6/7). The FORCEnet Warfare Sponsor is the Director of Space, Information Warfare, Command and Control Division (CNO N61). The FORCEnet Type Commander and Project Coordinator is the commander, Naval Network Warfare Command (NAVNETWARCOM). The FORCEnet Chief Engineer is the Commander, Space and Naval Warfare Systems Command (SPAWAR). Also intellectual investment will be continually provided by the Fleet, the Naval War College (NWC), the Navy Warfare Development Command (NWDC), the other systems commands and the Office of Naval Research (ONR).[57]

The priority implementation steps to put FORCEnet into play are; establishing open architecture systems and standards to allow rapid upgrades and integration; building common databases to widely share information; implementing standard user interfaces; and establishing portals to allow users to pull data from common servers.[58]

---

[57] Roche, Patrick. A FORCEnet Framework for Analysis of Existing Naval C4I Architectures. Master's Thesis, Naval Postgraduate School, Monterey, California, June 2003. p. 23.

[58] Ibid.

These implementation steps are intended to support the following FORCEnet objectives:

- *Enhance sensing, connectivity and decision- making*. This requires filling capability gaps to provide persistent intelligence, surveillance and reconnaissance; emphasizing rapidly deployable, distributed and networked unmanned systems; enhancing communication systems to optimize bandwidth and satellite resources; tailoring command and control systems to suit the new architecture; and making network infrastructures dynamic and interoperable.
- *Expand joint, interagency and coalition interoperability*. FORCEnet is intended to transcend organizational boundaries to integrate joint, coalition and interagency platforms, systems, networks and weapons, as well as non-governmental and international agencies when necessary.
- *Invest in intra-theater capabilities*. Communication paths frequently follow out-of-theater paths to in-theater destinations. This is inefficient and inconsistent with Sea Basing. Intra-theater capacity and capability will have to grow to optimize global resources as higher capacity systems emerge.
- *Focus on the "warrior" in FORCEnet development*. Improved human-system integration is central to realizing the potential that FORCEnet can bring to greater situational awareness, self-synchronized execution and faster speed of decision.
- *Experiment, innovate, integrate and implement*. The iterative nature of Sea Trial is the only viable option for implementing a concept as comprehensive and transformational as FORCEnet.[59]

FORCEnet is the Naval Forces "operational construct and architectural framework for warfare in the information age which integrates warriors, weapons, sensors, networks, command and control, and platforms into a networked distributed combat force, scalable across multiple levels of conflict from seabed to space and sea to land."[60] Transforming and developing FORCEnet will be challenging, not only because of the increasing complexity of technology, but also the integration that needs to occur across the different services.

[59] Ibid., pp. 23-24.

[60] Evans, Nicholas D. *Military Gadgets: How Advanced Technology Is Transforming Today's Battlefield...and Tomorrow's*. p. 226.

B. SEA POWER 21

Sea power 21 is one of the driving documents on the philosophy of integrating sea, land, air, space, and cyberspace in global joint operations against "regional and transnational dangers".[61] Essentially these are the driving tenants behind FORCEnet. Future naval operations will require information superiority to succeed and to gain this superiority will require a fully networked force. Sea Power 21 is a vision to transform our naval forces to achieve the above elements and defeat our enemies.

Sea Power 21 has three main elements: Sea Shield, Sea Strike and Sea basing. These three elements are the main enablers of FORCEnet, which integrates warriors, sensors, networks, command and control into a fully netted force.[62]

Figure 14. Sea Power 21[63]

[61] Sea Power 21. Proceedings, October 2002. Admiral Vern Clark. p. 2.

[62] Roche, p. 12.

[63] Ibid

Sea Power 21 will take advantage of America's increased computing power, systems integration, strong industrial base and its extraordinary service men and women.

1. Sea Strike: Projecting Precise and Persistent Offensive Power

The main focus of Sea Strike is naval power projection that will involve the dynamic application of intelligence, surveillance and reconnaissance. Information operations will play a critical role in Sea Strike; networked, long-dwelling sensors will be integrated with joint systems to provide precise targeting data, intelligence and control to every command level.[64]

- Sea Strike Impact
  - Amplified, effects-based striking power
  - Increased precision attack and information operations
  - Enhanced warfighting contribution of Marines and Special Forces
  - "24 / 7" offensive operations
  - Seamless integration with joint strike packages
- Sea Strike Capabilities
  - Persistent intelligence, surveillance, and reconnaissance
  - Time-sensitive strike
  - Electronic warfare / information operations
  - Ship-to-objective maneuver
  - Covert strike
- Future Sea Strike Technologies
  - Autonomous, organic, long-dwell sensors
  - Integrated national, theater, and force sensors
  - Knowledge-enhancement systems
  - Unmanned combat vehicles
  - Hypersonic missiles
  - Electro-magnetic rail guns
  - Hyper-spectral imaging
- Sea Strike: Action Steps
  - Accelerate information dominance via FORCEnet

[64] Roche. p. 14.

- Develop, acquire, and integrate systems to increase combat reach, stealth, and lethality
- Distribute offensive striking capability throughout the entire force
- Deploy sea-based, long-dwell, manned and unmanned sensors
- Develop information operations as a major warfare area
- Synergize with Marine Corps transformation efforts
- Partner with the other services to accelerate Navy transformation[65]

2. Sea Shield: Projecting Global Defensive Assurance

Sea Shield's main concept is to provide a layered defensive posture based on control of the seas, forward presence, and networked intelligence. Sea Shield will also allow the US to enhance homeland defense, assure access to the littorals (near land areas of the world which is any land or ocean within 650 miles (1046 km) of the coastline. This is equivalent to the furthest striking range of naval forces[66]), and project power deep inland.

- Sea Shield Impact
  - Projected defense for joint forces and allies ashore
  - Sustained access for maritime trade, coalition building, and military operations
  - Extended homeland defense via forward presence and networked intelligence
  - Enhanced international stability, security, and engagement
- Sea Shield Capabilities
  - Homeland defense
  - Sea / littoral superiority
  - Theater air missile defense
  - Force entry enabling
- Future Sea Shield Technologies
  - Interagency intelligence and communications reach-back systems
  - Organic mine countermeasures
  - Multi-sensor cargo inspection equipment

---

[65] Clark, pp. 13-14.

[66] Bowden, Scott. Forward Presence, Power Projection, and the Navy's Littoral Strategy: Foundations, Problems and Prospects. www.irisresearch.com/littorals.htm. July 31, 2004.

- Advanced hull forms and modular mission payloads
- Directed-energy weapons
- Autonomous unmanned vehicles
- Common undersea picture
- Single integrated air picture
- Distributed weapons coordination
- Theater missile defense

- Sea Shield: Action Steps

  Expand combat reach

  - Deploy theater missile defense as soon as possible
  - Create common operational pictures for air, surface, and subsurface forces
  - Accelerate the development of sea-based unmanned vehicles to operate in every environment
  - Invest in self-defense capabilities to ensure sea superiority[67]

3. Sea Basing: Project Joint Operational Dependence

Operational maneuver has always been the baseline for the U.S.'s military successes will continue to extend its reach with networks and sensors exploiting the largest portion of the earth; the sea. "Sea Basing serves as the foundation from which offensive and defensive fires are projected- making Sea Strike and Sea Shield realities".[68] With declining overseas bases and increased enemy access to weapons of mass destruction (WMD), it is to the US's advantage to expand our presence through mobile networked sea bases.

Sea Basing will give Joint Force Commanders global command and control capability which in turn can be used to give logistical support to other US forces or coalition partners. The Sea Based platform concept will increase the effectiveness of joint operations and also enhance coalition building efforts by sharing information and intelligence with other nations in times of crisis.

- Sea Basing Impact
  - Pre-positioned warfighting capabilities for immediate employment

[67] Clark p. 6.

[68] Ibid., p. 7.

- Enhanced joint support from a fully netted, dispersed naval force
- Strengthened international coalition building
- Increased joint force security and operational agility
- Minimized operational reliance on shore infrastructure

- Sea Basing Capabilities
  - Enhanced afloat positioning of joint assets
  - Offensive and defensive power projection
  - Command and control
  - Integrated joint logistics
  - Accelerated deployment and employment timelines
- Future Sea Basing Technologies
  - Enhanced sea-based joint command and control
  - Heavy equipment transfer capabilities
  - Intra-theater high-speed sealift
  - Improved vertical delivery methods
  - Integrated joint logistics
  - Rotational crewing infrastructure
  - International data-sharing networks
- Sea Basing: Action Steps
  - Exploit the advantages of sea-based forces wherever possible
  - Develop technologies to enhance on-station time and minimize maintenance requirements
  - Experiment with innovative employment concepts and platforms
  - Challenge every assumption that results in shore basing of Navy capabilities[69]

4. FORCEnet: Enabling the 21st Century Warrior

Sea Strike, Sea Shield, and Sea Basing are the concepts of Sea Power 21 and FORCEnet is the glue that holds all three together. FORCEnet is the "operational construct and architectural framework for Naval warfare in the information age".[70] FORCEnet will increase situational awareness by integrating systems, functions and

[69] Ibid., p. 8

[70] Naval Operating Concept for Joint Operations. www.mccdc.usmc.mil 31 July 2004. p. 4.

missions that will harness information for knowledge based combat operations. "It will also provide real-time enhanced collaborative planning among joint and coalition partners".[71]

FORCEnet will utilize integrated capabilities which include maritime information processing and command and control components that are interoperable with joint systems. These joint systems include intelligence, surveillance, and reconnaissance capabilities which aid in rapid targeting and maneuvering.

- FORCEnet Impact
  - Connected warriors, sensors, networks, command and control, platforms, and weapons
  - Accelerated speed and accuracy of decision
  - Integrated knowledge to dominate the battlespace
- FORCEnet Capabilities
  - Expeditionary, multi-tiered, sensor and weapons grids
  - Distributed, collaborative command and control
  - Dynamic, multi-path and survivable networks
  - Adaptive / automated decision aids
  - Human-centric integration[72]

C. NAVAL OPERATING CONCEPT (NOC) FOR JOINT OPERATIONS

Sea Power 21 was written mainly from a Navy point of view where the NOC for joint operations takes a look at joint operations in the eyes of the Navy and Marine Corps Team (the Naval Services). "In supporting our National Security Strategy, we assure allies, dissuade military confrontation, deter threats and coercion, and, when required, preempt or defeat our Nation's adversaries".[73]

The NOC for joint operations is a capstone concept that describes in broad terms how the Navy and Marine Corps team will operate across a full range of military operations. The NOC will integrate Navy and Marine Corps forces with the Army, Air Force and coalition partners for joint and multinational operations. "Many of the

[71] Clark p. 9.

[72] Ibid., p. 9.

[73] Naval Operating Concept for Joint Operations, p. 1.

traditional core characteristics of Naval Forces are intertwined with the Joint Force attributes described in the Joint Vision and emerging joint operating concepts. In addition the major components described in detail in this document integrate and incorporate elements of the joint concepts as indicated in Figure 15 below".[74]

Figure 15. Naval Operating Concept for Joint Operations[75]

The NOC is the basic architecture of how the Navy-Marine Corps Team operates. To meet the demands of the defense strategy, the Navy and Marine Corps must continue to operate effectively as a forward-postured, immediately employable force in joint and multinational environments. "The service visions, *Sea Power 21* and *Marine Corps Strategy 21*, recognize the challenges posed by a changing security environment and point the way to the future. Naval Services will organize, deploy, employ and sustain forces to conduct operations guided by the interrelated and complementary concepts of *Sea Strike, Sea Shield and Sea Basing* integrated with the family of Marine Corps concepts, *Expeditionary Maneuver Warfare, Operational Maneuver from the Sea,* and *Ship-to-Objective Maneuver*; all of this will be enabled by *FORCEnet*".[76] (These concepts and terms are explained in the Figure 16.)[77]

[74] NOC, p. 3.

[75] Ibid

[76] Ibid.

[77] Ibid.

- ***Sea Strike*** is a broadened concept for projecting precise and persistent Naval offensive power. It describes how 21st-century Naval Forces will exert direct, decisive, and sustained influence in joint campaigns through the application of persistent intelligence, surveillance, and reconnaissance (ISR), time-sensitive strike, *Ship-to-Objective Maneuver (STOM),* and information operations (IO) to deliver accurate and devastating combat power.
- ***Sea Shield*** is a concept that describes the manner in which Naval Forces will protect our national interests with layered global defensive power. It is based on our sustained forward presence, and on our abilities to dominate the seas and to provide distributed and networked intelligence to enhance homeland defense, assure access to the contested littorals, and project defensive power deep inland.
- ***Sea Basing*** serves as the foundation from which offensive and defensive power are projected, making *Sea Strike* and *Sea Shield* realities. It describes the projection, sustainment, and operational maneuver of sovereign, distributed, and networked forces operating globally from the sea. *Sea Basing* will provide Joint Force Commanders with global command and control (C2) capability and extend integrated support to the other Services.
- ***Expeditionary Maneuver Warfare (EMW)*** will serve as the Marine Corps capstone concept for the 21st century. It is the union of Marine Corps core competencies, maneuver warfare philosophy, and expeditionary heritage.
- ***Operational Maneuver from the Sea (OMFTS)*** is a concept for the projection of maritime power ashore. It focuses on the operational objective using the sea as maneuver space and pitting strength against weakness. It generates overwhelming tempo and momentum; it emphasizes intelligence, deceptions, and flexibility; and it integrates all organic, joint, and multinational assets.
- ***Ship-to-Objective Maneuver (STOM)*** applies the principles and tactics of maneuver warfare to the littoral battlespace. It allows for conducting combined arms penetration and exploitation operations from over the horizon directly to objectives ashore without stopping to seize, defend, and build up beachheads or landing zones.
- ***FORCEnet*** is the enabler of these capabilities, and the operational construct and architectural framework for Naval warfare in the information age. It will allow systems, functions, and missions to be aligned to transform situational awareness, accelerate decision making, and allow Naval Forces to greatly distribute their combat power.

Figure 16. Integration of Sea Power and Marine Corps Strategy 21

D. THE STRATEGIC STUDIES GROUP (SSG)

1. Strategic Studies Group History

The Strategic Studies Group (SSG) was founded in 1981 by Admiral Thomas Hayward, the Chief of Naval Operations (CNO). The SSG resides at the Naval War college (NWC) in Newport, Rhode Island. The CNO personally selects Fellows from the Navy, Marine Corps and the Coast Guard to work on its sole mission: the generation of revolutionary naval warfare concepts. These concepts are developed by:

- Exploring innovations in naval warfighting
- Developing warfighting concepts,
- Underpinning these concepts with technologies,
- Establishing criteria to evaluate these concepts in operational experiments, and

- Recommending actions directly to the CNO.[78]

Over the course of several years the SSG has come up with the concepts that comprise the majority of the framework for Sea Power 21 and FORCEnet. The naval forces will need FORCEnet in order for the military to transform into a more adaptive and knowledgeable force. FORCEnet will aid in this transformation while delivering an increase in combat power. The SSG has devised a blueprint overview and an architecture to bridge the gap between legacy systems of today with a fully networked force.

- Blueprint Overview
  - **Block I** – Block I will necessarily be populated with systems that are in the fleet today, netted together using current technology and human performance considerations. The SSG believes it will be attainable by 2006. The primary purpose of Block I is to, at a basic level, net the naval force in order to realize an initial operational capability. This initial capability will allow experience to be gained in order to support operational, organizational, and technical decisions to be made in preparation for subsequent blocks.
  - **Block II** – Block II will be designed, built, and delivered to the fleet—fully netted and fully integrated—with human performance woven into the process. Block II can be achieved in 2010.
  - **Block III –** Block III will include substantial enhancements beyond Block II. Its design and developmental process will be wedded to the Human System Integration process, resulting in a truly human-centric architecture and an ongoing spiral development of warfighting capabilities. Block III can be operational by 2020.[79]

[78] CNO SSG XIX, Naval Power Forward, p. xiii.

[79] CNO SSG XX, p. 2-1.

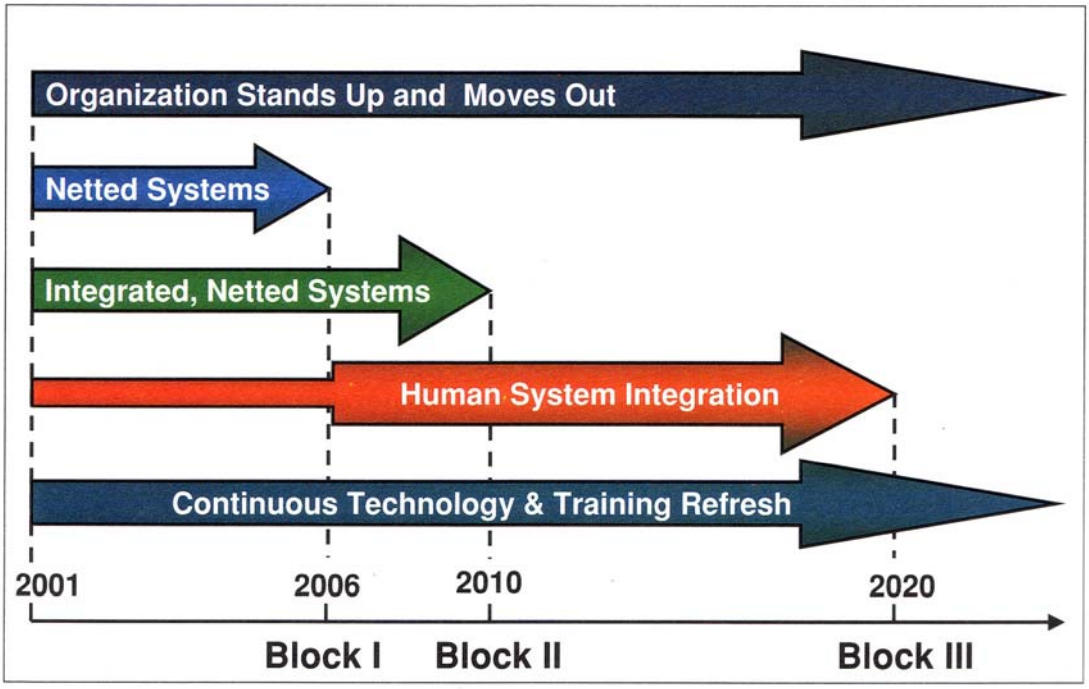


Figure 17. Blueprint Overview[80]

The inability of Industrial Age organizations to compete in the Information Age is that they are not effective in taking advantage of the information and expertise that is available to them. They are still stuck somewhere in the lower left quadrant of the transformation graph that has been repeatedly been referred to throughout this thesis. What the SSG has endeavored itself to do is to provide a timeline to incorporate Sea Power 21 to further move it to the upper right hand of the chart. What the SSG realized is that transformation can not be accomplished overnight and goals must be set and establish a blueprint to chart a course for it to follow.

[80] Ibid.

V. TRIDENT WARRIOR 03 EXERCISE

A. TRIDENT WARRIOR 03 BACKGROUND AND OVERVIEW

Trident Warrior 03 (TW03) was conducted 25-30 September 2003 with the USS ESSEX Expeditionary Strike Group (ESG). The ESSEX ESG contained elements of Amphibious Squadron Eleven, the 31st Marine Expeditionary Unit (MEU), and the USS Chancellorsville. The mission of TW03 included:

- ESG Limited Objective Experiment (LOE) that focused command and control issues for the forward deployed Naval forces' (FDNF) ESG. TRIDENT WARRIOR 03 was also conducted in conjunction with the JTF WARNET Pre-Deployment Exercise (PDX).
- Integrated Prototype Demonstration (IPD) of an integrated prototype capability that fielded a supportable incremental delivery of FORCEnet capability.[81]

TW03 was a Naval Network Warfare Command (NAVNETWARCOM) and COMPACFLT sponsored event. NAVNETWARCOM and the Navy Warfare Development Command (NWDC) sponsored the ESG LOE. SPAWAR was the executing agent for the TW03 and the FORCEnet IPD and NWDC were the executing agent for the ESG LOE. The ESG LOE was comprised of three experimentation initiatives. NWDC led an initiative to refine ESG command and control (C2) Concept of Operations (CONOPs) and tactics, techniques, and procedures (TTP) for the ESG commander and his staff. Expeditionary Warfare Training Group Pacific (EWTGPAC) led an initiative addressing ESG fires CONOPs and TTP. Third Fleet's Network Centric Innovation Center (NCIC) led a third initiative assessing the implementation of information management and knowledge management techniques.[82] A graphic depiction of the event is shown in Figure 18.

[81] Trident Warrior 2003 Analysis Report. p. 15.

[82] Ibid.

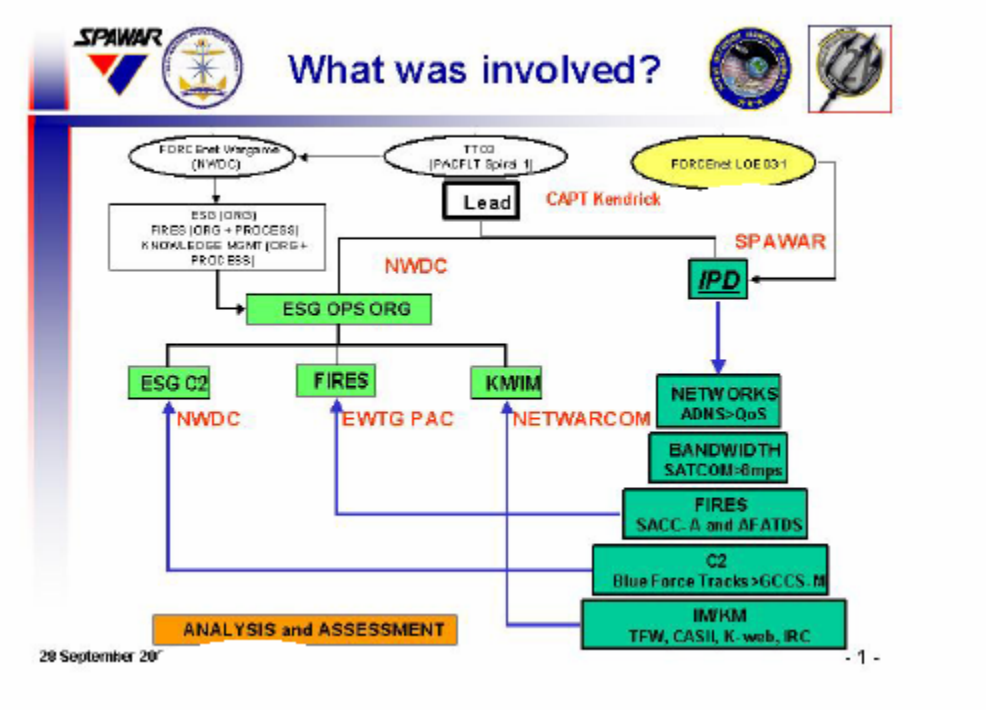


Figure 18. Overview of TW03[83]

TW03 was conducted in conjunction with the ESG Limited Objective Experiment (LOE) and the Joint Task Force wide-area relay network (JTF WARNET) Pre-Deployment Exercise (PDX). External to TW03, but in competition for critical shipboard resources, a Special Operations Capable Exercise (SOCCEX) was conducted during the first three days of the experiment.

The three major FORCEnet capabilities that were the focus of the experiment were:

- Dynamic, multi-path, survivable networks
- Distributed, collaborative command and control
- Expeditionary, multi-tiered sensor and weapon information.

The author will take an in-depth look at each of the capabilities and provide an overview of the capabilities' successes and failures.

B. DYNAMIC, MULTI-PATH, SURVIVABLE NETWORKS

TW03 made substantial progress in the advancement of network infrastructure. The stated goal for TW03 was to provide the warfighter with a dynamic, multi-path and

[83] Ibid.

survivable network core infrastructure. The technical areas to support this FORCEnet capability are as follows:

- Improved routing architecture
- Line of sight networking enhancements
- QoS implementation
- Increased Capacity

1. Improved Routing Architecture

The Navy has been evolving its mobile routing architecture for over a decade within the ADNS program. The Navy uses its mobile IP routing architecture to provide network connectivity to afloat units deployed worldwide. USMC forces interface with the Navy's IP infrastructure using the MAGTF router, configured to provide gateway services on amphibious platforms to support USMC forces afloat. The USMC forces transition to a stationary routing structure when they go ashore.

The Navy has developed and fielded a revised routing architecture designed to take advantage of recent bandwidth increases and commercial router enhancements and to improve routing flexibility and performance. The updated routing architecture enables mobile, self-forming networks among ships, across AORs, by modifying the autonomous system structure. The revised architecture leverages commercially available technology in a configuration that allows it to adapt to the connectivity available in the local area. The resulting self-forming, ad hoc network improves flexibility, survivability, and availability of the warfighting networks without increasing the complexity presented to the operator. While still in the early stages of development, these advances are a key component in the DoD's network centric warfare capability.

The improvements made to the ADNS routing architecture had extremely positive results on operational performance. A principal goal of ADNS is to develop effective and efficient shipboard and shore-based systems that maximize the amount of IP data transported over RF links allocated for ADNS management.[84]

2. Line of Sight Networking Enhancements

During the Integrated Prototype Demonstration (IFD), two Line Of Sight (LOS) networks were integrated to establish a seamless, high-bandwidth theater networking

[84] Ibid., p. 33.

capability not previously available. The Intra-Battle Group Wireless Network (IBGWN) and the Joint Task Force Wide Area Relay Network (JTFWARNet) are based on the VRC-99 radio, considered a JTRS surrogate, and Cisco® routing technology. Beyond LOS, capability can be achieved for both networks using fixed or rotary wing airborne relays.

The IBGWN networks Naval forces that are within LOS proximity. It allows members to access services and provides reach back capability throughout the ESG. Members use the naval routing and addressing schema. The radios work in conjunction with ADNS to provide network connectivity to what were formerly SATCOM disadvantaged platforms.

Some of the most impressive TW03 results were the network and operational advantages enabled by the introduction of the LOS networks IBGWN and JTFWARNet. JTFWARNet was participating in TW03 as part of their pre-deployment exercise and will be publishing a separate report with an extensive analysis of that system. The analysis focus for this report will then be on IBGWN.[85]

3. Quality of Service (QoS)

Quality of Service (QoS) is a key enabler for the migration of legacy applications to the network. Many applications have deterministic expectations of host networks not supported in the previous network configurations, requiring those applications to maintain independent, stovepipe communications architectures. With QoS, the Navy expects to be able to collapse application stovepipes and optimize the total bandwidth among network application users.

For the IPD, QoS was implemented using a two-step process. The application data flows were classified and marked by a PacketShaper® device integrated with ADNS, a system developed to explicitly tag individual data flows emanating from applications residing on the shipboard LANs. The second step in the process was to route the data flows, based on the PacketShaper® marking, to the appropriate queues. ADNS supported four queues for priority and output queues for the wide area connectivity including CA-III, and SHF.

[85] Ibid., p. 36.

During TW03, the increased bandwidth capacity provided for the experiment exceeded demand and congestion was not observed. Thus, while traffic was classified and marked by the PacketShaper®, QoS was not really required due to a lack of demand, and therefore, prioritization queuing was not observed.

QoS as implemented for TW03 only affected traffic leaving the ship. It is normally traffic inbound to the ship that causes congestion, however, as inbound traffic normally far exceeds outbound traffic. QoS for traffic inbound to the ship would have to be implemented at the Network Operation Center (NOC). During TW03, there was no QoS for traffic inbound to the ship, but ADNS has plans to start implementing QoS from the NOCs in FY-04.[86]

4. Increased Capacity

The bandwidth connecting the ESG to the wide area network was expanded during the experiment. Both the WSC-8 and WSC-6 were upgraded to include all current engineering and field changes. The Commercial Wideband Satcom Program (CWSP) throughput was increased from 2 Mbps to 4 Mbps using a commercial cell multiplexer. The WSC-6 (V)5 supported one of the carriers for a maximum total WSC-6 throughput of 2 Mbps. The resulting capability was a combined throughput of up to 6 Mbps supporting SCI, secret, and unclassified IP data, secure and non-secure telephones, and legacy serial feeds.

In addition to SATCOM's increased bandwidth, the IBGWN LOS networks implemented for TW03 also had the effect of increasing available bandwidth, as discussed previously in this report. The increased overall capacity essentially made bandwidth a non-issue for USS *Essex* during TW03.

It was noted, however, that there are technological impediments to utilizing large amounts of bandwidth. JCA appeared to be the only application capable of fully utilizing the available bandwidth. JFN, for instance, peaked at approximately 150 kbps, sometimes leaving over 500 kbps of capacity unused. This may be an artificiality associated with the use of the typical landline link TCP over satellite links.

[86] Ibid., pp. 39-40.

As more satellite bandwidth becomes available, it is important that applications, operating systems, and servers be developed with due consideration to end user operational conditions, including latencies associated with SATCOM. Systems that perform well on terrestrial networks may perform quite differently across satellite networks.[87]

Tables 1-4 summarize the network improvements made during the TW03 exercise.

Table 1. Summary of USS Fort McHenry Network Improvements

Measure		Before (satcom only)	After (w/ LoS networks and ADNS upgrade)	Percent change
Throughput	Inbound	20.0 kbps	25.8 kbps	29% increase
	Outbound	59.0 kbps	67.1 kbps	14% increase
Availability	Inbound	87.7%	99.4%	13% increase
	Outbound	86.0%	99.2%	15% increase
Total Outage Time per Day	Inbound	2 hrs 57 min	9 min	95% reduction
	Outbound	3 hrs 22 min	12 min	94% reduction
# of Outages		23	2	91% reduction
Avg Outage Duration	Mean	12 min 16 sec	3 min 12 sec	74% reduction
	Max	2 hrs 19 min	6 min	96% reduction

Table 2. Summary of USS Essex Network Improvements

Measure		Before (satcom only)	After (w/ LoS networks and ADNS upgrade)	Percent change
Throughput	Inbound	134.0 kbps	148.6 kbps	11% increase
	Outbound	54.9 kbps	63.3 kbps	15% increase
Availability		98.9%	99.8%	1% increase
Total Outage Time per Day		15 min 56 sec	2 min 12 sec	86% reduction
# of Outages		5.75	4.5	22% reduction
Avg Outage Duration	Mean	2 min 46 sec	29 sec	82% reduction

[87] Ibid., p. 40.

Table 3. Summary of USS Chancellorsville Network Improvements

Measure		Before (satcom only)	After (w/ LoS networks and ADNS upgrade)	Percent change
Throughput	Inbound	155.8 kbps	191.1 kbps	23% increase
	Outbound	104.4 kbps	118.9 kbps	14% increase
Availability		96.3%	98.7%	2% increase
Total Outage Time per Day		53 min 52 sec	19 min 25 sec	64% reduction
# of Outages		8	6	25% reduction
Avg Outage Duration	Mean	9 min 15 sec	3 min 56 sec	57% reduction

Table 4. Network Reliability Improvements with IBGWN and ADNS upgrade[88]

Ship	With own SATCOM only		With IBGWN and ADNS upgrade	
	Availability	Daily outage time	Availability	Daily outage time
USS *Fort McHenry*	86%	3 hrs 22 min	99.2%	12 min
USS *Essex*	98.9%	15 min 56 sec	99.8%	2 min 12 sec
USS *Chancellorsville*	96.3%	53 min 52 sec	98.7%	19 min 25 sec

5. Overview of TW03 Network Successes and Failures

Packetshaper, a traffic management system that monitors application performance over the network and the Advanced Digital Network System (ADNS), provided substantial increases in the quality of service (QoS) and increased throughput throughout the network. The USS Ft. McHenry improved network availability from 86% to 99.2%, throughput increased over 17%, outages were reduced by 91% and the mean duration of outages dropped 74%.

The Intra-Battle Group Wireless Network (IBGWN) was a huge success in that it demonstrated its high value to net-centric operations. IBGWN proved to be invaluable by providing an alternate route for IP traffic when normal traffic across SATCOM links failed.

The performance of the integrated network operations technologies was satisfactory. The combination of the inter-battle group wireless network (IBGWN), quality of service (QoS) software and automatic digital network system (ADNS) was

[88] Ibid., pp. 39-40.

viewed by ESG as a noticeable increase in efficient bandwidth management capability. The ability to exchange information over a line of sight wireless local area network between ESG units was observed as a major increase in capability.

Blue Force Tracking (BFT) did not perform as expected, and was the biggest disappointment within the technology systems area. This failure, however, was apparently due primarily to an incompatibility internal to the shipboard computers that precluded successful data management. It cannot be concluded that the BFT system will not work or how well it might work; just that it did not work during TW03. Additional testing and evaluation is needed on this system before any definitive conclusions can be reached.[89]

C. DISTRIBUTED, COLLABORATIVE COMMAND AND CONTROL

Robust networks are a key enabler of FORCEnet. The vision is to "transform situational awareness; accelerate speed of decision making, and to greatly distribute combat power."[90] The following TW03 focus areas directly support this FORCEnet capability:

- Situational awareness (SA) enhancements
- Collaboration enablers
- Information management and knowledge management[91]

There were significant gaps in shared situational awareness for TW03. One of the biggest factors is the time latency issues associated with the Global Command and Communication System- Maritime (GCCS-M). The following SA examples are taken from the TW03 Summary Analysis Report:

> 1. Common operational picture (COP) requires a more timely C2 system onboard the ESG flagship. Without additional adequate C2 support in this area, it would either force delegation of real-time control to a platform with real-time C2 systems (e.g., Aegis cruisers and destroyers) or an improved C2/LINK-16 suite on USS *Essex* and other ESG flagships. GEOVIZ hardware requirements were supported in only four out of 300+ computers on USS *Essex* due to the age of the Integrated Shipboard Network System (ISNS) personal computers (PCs) (the shortfalls were in computer memory and video card memory). WebCOP (with imagery,

[89] Ibid., pp. 2, 3.

[90] Clark, Vern. Sea Power 21, Part I. U.S. Naval Institute Proceedings, October 2002.

[91] Trident Warrior 03 Summary Analysis Report, p. 3.

weather, etc, overlays) was available to any SIPRNET user with a browser. Tactical Action Officers (TAOs) displayed flexibility by relying on less technical methods to maintain the tactical COP (e.g. paper and pen or powerpoint charts with scenario maps). Because the COP contained both real and simulated tracks, it was quite cluttered and difficult to understand.

2. There were critical breakdowns in shared situational awareness that require attention. The information management (IM) plan and integration of CWC and ARG/MEU operations that were implemented in the ESG LOE did not effectively support all of the required decision-making. Examples include the inability of GREENCROWN (on USS *Essex*) to manage airspace deconfliction due to the lack of a real-time air picture and the inability of the ESG Commander to exercise command by negation for fires processed by the Force Fires Coordination Center (FFCC) / Automated Supporting Arms Coordination Center (SACC-A). In the case of GREENCROWN, there is a time latency limitation to the current battle management system (Global Command and Control System - Maritime; (GCCS-M)) which limits the quality of the data used to manage airspace. However, with respect to the SACC-A the issue involves a lack of connectivity and procedures between command and control nodes (and the people manning those spaces) that have not historically had to interact.

3. Situational awareness is a continuing process and the limitation of reliance on chat as a status indicator was highlighted when one shooter was not aware that he was supposed to be in position to provide fire support to shore. Design of a tool that provides support to users in the form of process status indicators that augment the collaborative message content would help avoid some of these situation awareness problems.

4. The Battle Watch Commander (BWC) had no means of documenting his thoughts other than by dictating to the Strike Watch Officer (STWO), who also monitored three chat rooms, email, and two web sites. Thus, much of what the BWC discussed on the watch floor was lost because of the inability to document it efficiently.[92]

Collaboration enablers are the primary foundation which provides SA. The following observations were made:

1. Internet protocol (IP) chat in one form or another has become central to collaboration. No standard chat program is used between services. Depending on the program in use, there are variances associated with the number of users accommodated; the number of chat programs able to be displayed; the training provided beforehand on the software; the ambiguity of operating procedure descriptions; and challenges to operators in

[92] Ibid., p. 4.

monitoring the relevant chat networks. There are technical design incompatibilities between different chat programs. Another consideration was observed in Fleet Battle Experiment – Kilo, the IWS chat program can use over 25 times as much bandwidth as the mIRC chat program.[93] In TW03, three different chat programs were used and the services attempted to change programs to match other services with whom they were coordinating – with mixed results. Icorps and the 25th ID could not chat with CESG due to incompatible chat standards. The U.S. Army uses IWS and the USN/USMC use the chat standard embodied in the IT21 system. Clearly, efficiency could be improved by using one chat program that embodied optimal characteristics (as defined by FORCEnet) of those presently available in the commercial or freeware marketplace.

2. The chat system was also limited by the synchronous nature of the system that required constant attention to monitor communications, by the number of participants that could be accommodated and recognized, and by the time required for users to authorize, compose, and type messages.

Although the chat system proved adept at exchanging focused information in real time, it was not up to the task of logging transient information in a way that could be used to indicate process status or queried for specific content.

3. Multiple ESG collaborative websites existed but because procedures for posting critical information to these sites were not evident, collaboration was inhibited.

4. Because of the concurrent events during TW03, three different chat tools were available for use by the watch stander. Besides the IMP, which was not widely read, there was little guidance and training provided on which system to use during a particular event. Operator's were confused and worked almost exclusively with current IT21 tool suite (Microsoft chat), reducing any advantage the other systems may have offered. I Corps and 25th ID could not chat with CESG due to incompatible chat standards. The U.S. Army uses IWS and USN / USMC uses IRC standard chat resident on IT21 system. The Army using a commercial mIRC product mitigated this for this experiment.

5. HSI analysts concluded that C2 / collaboration technologies supported task performance and the attainment of experiment objectives, but various problem areas were noted. These included chat deficiencies described above, COP inconsistencies, and non-standard procedures and processes. Ergonomic deficiencies in the flag plot workspace layout were also noted. Although information transfer was improved, problems were also noted in adequately monitoring tasking, scheduling, and critical events; identifying scheduling and resource conflicts; and tracking progress toward

[93] Fleet Battle Experiment–Kilo Network Analysis. Naval Postgraduate School. May 2003.

> objectives. Training was marginal, resulting in users being unaware of numerous features of the technologies. Documentation and online help need to be improved for most C2 / collaboration technologies.[94]

Information management and knowledge management results from all analysts involved in the ESG LOE clearly recognize that the information management was insufficient. From an information management plan (IMP) standpoint, network operations were deemed fully mission capable, although additional improvement is possible. The ability to use net-centric warfare (NCW) processes to move information from node-to-node was observed to be poorly executed by the ESG. The critical/non-mission capable areas include C2/collaboration information transfer and training. The maturity of the ESG in using NCW concepts was not up to speed for even intermediate application of NCW techniques. All other areas were deemed partially mission capable and require substantial modifications to processes and implementation to reach a fully mission capable status. Observational data suggests that the following are contributing factors:

1. The ESG is made up of units unfamiliar with working with each other.

2. Although the LOE provided an abundance of new collaboration methods, the participants tended to withdraw toward what they knew how to operate, possibly due to insufficient training.

3. Although an IMP was provided and briefed to the senior ESG staff, most of the participants did not have a reasonable level of familiarity with the plan.

4. The scope of the IMP did not have universal agreement. The IMP provided to the ESG by NCIC focused on providing instructions to participants about the methods to operate individual systems within the LOE. While this clearly meets the test of "necessary," it is not "sufficient" for complete information management. This requires an IMP that follows functional paths that cross through individual system paths. In other words, from an operators view, information management requires the who's, what's, when's, and how's. The IMP developers expected this guidance to come from the ESG staff. Unfortunately, there is no doctrine that lays out what the content of a IMP should be.

5. Generally, the ESG staff, PWC, and ship's personnel did not read the IMP. The IMP was briefed to COs and staff and it was noted that barely

[94] Trident Warrior 03 Summary Analysis Report. p.4-5.

anyone below the rank of CDR (O-5) read the IMP. For those who did read the IMP, they generally had a very good understanding of how to use IM systems in their processes.

6. The IMP and integration of CWC and ARG/MEU operations implemented in the ESG LOE did not effectively support all required decision-making. LOE observers on USS *Essex* noted that the primary collaboration method was via radio telephone (R/T), and that chat was the secondary method. However, analysts on USS *Chancellorsville* observed that chat was the primary collaborative tool and that the watchstanders complained about the ESG / USS *Essex* not being up on R/T circuits. This variability highlights the disparity in IM practice across the ESG.[95]

D. EXPEDITIONARY, MULTI-TIERED, SENSOR AND WEAPON INFORMATION

The digital architecture configured for TW03 (ESG LOE/FORCEnet IPD) efficiently passed data required to conduct ISR/collections management and target engagement execution. Objective data analysis shows that targeting information required to utilize digital tools to ultimately put a weapon on target quickly was accomplished. TW03 demonstrated that the digital network was in place to perform rapid target execution but the organization and decision-making systems and processes needed to effectively execute engagement of targets in a timely manner were not.[96]

Fires observations and analyses of data focused on four primary areas: Fires Coordination Process, Fires Execution Process, Fires Execution Systems and Fires from the Human Systems Integration perspectives. Below are some of the key findings from the TW03 Analysis report.

1. Fires Coordination Process

1. From a fires perspective, the TW03 goal was to focus on unique aspects of ESG operations and specifically coordination with force fires execution that are not currently addressed in existing doctrine including organization, manning, staff responsibilities/functions, command relationships, employment issues, and training. However, ESG guidance for the Strike Warfare Commander (STWC) and interaction between the ESG and the Force Fires Coordination Center (FFCC) was virtually non-existent. Neither CONOP's nor Techniques, Tactics and Procedures (TTP's) were developed prior to experiment start nor was communication between ESG staff, STWC, and FFCC was observed to be very limited.

[95] Ibid p.5-6

[96] Ibid. p.7

Interviews and participant surveys indicate that strike efforts in FFCC were not coordinated with any ESG guidance. And, Post experiment analysis indicates that distributed Collaboration via Chat, Voice, or other between ESG, STWC, or Force Fires Coordinator did not occur.

2. ESG staff did not have standard operating procedures (SOPs) that would have established command and control process between ESG organization, STWC, and FFCC prior to experiment start. ESG and FFCC targeting priorities and strike decision-making process were disconnected throughout the effort.

3. Analysis results indicate that there was little interaction between the ESG, STWC, and FFCC regarding the prosecution of targets. The FFCC operated essentially autonomously. Although STWC did not receive clear fires direction from CESG during the experiment, he initiated targeting priorities and directed his Force Fires Coordinator to develop procedures and execute with existing MEW personnel and new SACC-A tools. This permitted operator's opportunity to explore new capabilities and provide feedback through interviews and participant surveys.

4. During ESG LOE, the Force Fires Coordination Center organization was not staffed to support concurrent current operations and future planning. It was observed that current operations ceased when any future planning meetings were conducted. The daily targeting board, for example, occupied the entire FFCC staff and impacted the current fight.[97]

2. Fires Execution Process

1. The operation of the FFCC centered on the AFATDS application for processing CFF originating with AFATDS and ADOCS for managing Time Sensitive Targets (TST's) originating with RTC in the JIC. It should be noted that the capabilities of ADOCS and AFATDS are similar except that AFATDS is capable of technical fire direction, which ADOCS is not. In this experiment, the AFATDS in the FFCC was not required to perform this role.

2. On USS *Essex* there were two RTC servers, one in the FFCC and one in the Sensitive Compartmented Information (SCI) area of the JIC. The former server had two clients in the JIC and one in the FFCC. The SCI RTC was not used in the experiment. The RTC workstation in the FFCC was used primarily to alert the Force Fires Coordinator that a nomination was being sent from the JIC, which it did effectively. The Advanced Field Artillery Data System (AFATDS) had no alert mechanism to indicate the arrival of a Remote Terminal Capability (RTC) target nomination (unlike Calls For Fire (CFF)), which could cause prosecution delays during real world, high op-tempo environments.

[97] Ibid., p. 24.

3. Battlespace shaping involves JTF or ESG tasking aimed at achieving a desired end state. The CESG was responsible for identifying battlespace shaping goals and direction for each PWC to help attain. Although observing battlespace shaping process was an objective of the ESG LOE, observations, interviews, and participant surveys clearly indicate that battlespace shaping for the fires mission area did not take place during the ESG LOE.[98]

3. Fires Execution System

SACC-A

1. The Supporting Arms Coordinating Center – Automated (SACC-A) architecture, systems, and TTP established during this experiment provided the capability to satisfactorily synchronize TST engagements and calls for fire.

2. The TW03 fires initiative did very successfully demonstrate Joint Interoperability. The Joint AFATDS in USS Essex Supporting Arms Coordination Center (SACC) very successfully communicated digital calls for fire (CFF) with the Naval Fires Communication System (NFCS) aboard USS *Chancellorsville*, and the NFCS very successfully reported CFF mission completions to AFATDS. However, The TW03 fires initiative did not demonstrate a FORCEnet digital end-to-end fires capability. It is not possible with the Mk-86 gunfire control system on AEGIS cruiser because NFCS does not have any interfaces with the Mk-86 gunfire control system. The digital train stopped at the NFCS terminal.

ADOCS

1. Automated Deep Operations System (ADOCS) provided good situational awareness for conducting TST operations as indicated in participant surveys. ADOCS was loaded on all RTC's, which provided Situational Awareness (SA) to the JIC including confirmation that their nominations were successfully received in the SACC.

2. ADOCS ability to rapidly locate target on imagery provided rapid method of approximating target position.

3. Clearance of TST engagements and CFF appeared to be timely and accurate using ADOCS and AFATDS.

AFATDS

1. Advanced Field Artillery Tactical Data System (AFATDS) provided the basic situational awareness to deliver fires ashore. When coupled with EMT/C2PC, the integrated system provided a real time projection of the

[98] Ibid., p. 25.

forces ashore thus making the deconfliction process manageable and permitting accurate and timely weapons on target.

2. AFATDS inability to process CIB imagery did not allow for more than map representation of the terrain.

3. The AFATDS had no alert mechanism to indicate the arrival of a Joint Fires Network JFN) Remote Terminal Capability (RTC) target nomination (unlike Calls For Fire (CFF)).

EMT

1. Effects Management Tool (EMT) was a critical component in the target engagement process. EMT rendered AFATDS tactical objects to its map and also permitted manipulation of these objects. This allowed the depiction of unit symbols registered to the correct location on the map, accurate placement of battlefield geometries and fire support coordination measures, and display of target symbols. EMT allowed for data drill down on the displayed objects that indicated information maintained within AFATDS.

NFCS

1. Naval Fires Control System (NFCS) has an automated interface with AFATDS – which provided joint interoperability with Army and Marine field artillery. This had an obvious benefit within an Expeditionary Strike Group for the Supporting Arms Coordination Center in that the SACC could pass missions electronically to the NSFS platform using the same fires command and control system for naval fires as for ground fires.

2. From USS *Chancellorsville*'s perspective, the FORCEnet IPD did very successfully demonstrate Joint Interoperability. The Joint AFATDS in USS *Essex* SACC very successfully communicated digital calls for fire (CFF) with the NFCS aboard USS *Chancellorsville*, and the NFCS very successfully reported CFF mission completions to AFATDS.

3. When opportunities did occur, several call-for-fire missions were successfully sent from AFATDS to NFCS aboard USS *Chancellorsville.* The missions were very effectively received, parsed, electronically processed inside NFCS, and displayed to the NFCS operator. NFCS also electronically reported fires mission completions back to AFATDS.

4. NFCS has a built-in capability to import data from GCCS. With this data plus any Fires Support Control Measures (FSCMs), NFCS has an automated capability to red-flag fires missions that might result in a blue-on-blue engagement, thus providing a two-dimensional deconfliction capability at the target area. All of the seven CFF missions conducted had no conflicts (i.e., no blue forces at risk), which NFCS reported to the

operator. There were no demonstrations of prevention of a blue-on-blue engagement.[99]

4. Fires from the Human System Integration Perspective

From a human-systems integration (HSI) standpoint, the technologies in the call for fires (CFF) process and the network operations generally supported the performance of the CFF activities. Particularly noteworthy were the reliability of operations and the ability to provide task-relevant information in a readily understood and easily assimilated format. However, difficulties were encountered when tracking critical events, monitoring the status of system users, resolving scheduling and resource conflicts, and transferring information between locations (e.g., SACC and ESG). Also, targeting information was not always sent to the Flag Plot, which impaired the situation awareness of the watch team. The HSI analysts concluded that training was marginal to insufficient and manpower was only one-deep for most Call for Fire (CFF) technologies. To mitigate risk of failure within this process, more extensive training is required.[100]

The following areas needed additional attention and consideration:

1. The connections between the fire control systems allowed users to share common situation awareness on tracks, targets, and fire schedules but were mediated by the GCCS-M position information, which could lag up to 15 minutes behind real-time. That lag is not good enough for some time-sensitive targeting tasks and can lead to a shared, but incorrect, awareness of target positions.

2. The utility of the links between the fire support systems were limited by the inability of AFATDS to accommodate the same target designations as ADOCS and by the lack of connection between the NFCS and the shooters weapon systems. These problems were circumvented by the operators who entered incorrect data into the systems that allowed the support systems to be used locally, but had the unfortunate result of sharing the incorrect data with other members of the Call for Fire (CFF) chain who then assumed that specified targets had not been engaged and issued redundant engagement orders.

3. The distribution of tasks between disjoint individuals in the CFF sequence tends to slow down the CFF process to accommodate the additional information transfers and verifications required to validate the target and synchronize the distributed CFF components. FORCEnet

[99] Ibid., pp. 25, 26.

[100] Ibid., p. 8.

technologies allowed many of the time-sensitive validation and deconfliction tasks in the CFF sequence to be performed rapidly, but were not well enough integrated with CFF workflow to show the operators the status of the information transfers between the tasks.

4. While the systems contained a great deal of information, operators often had difficulty locating critical information, such as ROE and message formats. This led to excessive delays in transmitting information and orders.

5. Display configurations and workspace layouts were problematic and led to inefficiencies in the way that information was transferred within and between command centers. Consideration of the proper location of operator workstations, legibility of shared displays, and easy access to task-relevant information would improve operations.[101]

E. GENERAL OBSERVATIONS OF TW03

In an interview with Dr. Shelley Gallup, a professor at the Naval Postgraduate School and one of the coordinators for TW03 on the operational side, Dr. Gallup summarized the experiment in one phrase; "TW03 was a technical success, but an operational failure".[102] Dr. Gallup further clarified his position by stating that the networking and the technical aspects (such as the IBGWN wireless network) were a huge success for TW03, but a lack of clarity of requirements on the experimentation side left much to be desired on the overall effectiveness of the mission.

Dr. Gallup also stated that limited funding played a big part in the inability to resolve some issues. In all, the Navy spent about $1.5 million on TW03; a small price to pay for what the Navy says is the "backbone" (FORCEnet) of Sea Power 21. Dr. Gallup also mentioned that an alignment of efforts or cross-domain solutions is required for many of the issues arising with FORCEnet. In other words, the Naval forces need to cut across organizational bureaucracies and cultural military barriers if FORCEnet is truly going to be interoperable with all the services throughout the military. He also stated that many of the issues documented for TW03 have been addressed for the TW04 exercise. Table 5 is a summary of the FORCEnet Functional Capabilities for TW03.

[101] Ibid., p. 9.

[102] Gallup, Shelley. Interview with author. July 16, 2004.

Function	Sub-Functions	Command and Control	Fires	IM/KM	HSI	Technology	METOC
Expeditionary, multi-tiered sensor and weapon info							
	Collect, Process and distribute organic sensor and weapon info	N/A	No real sensors and no sensor management in ESG LOE.	Limited success, but no standard procedures for distribution of info by either website or standard collaborations.	N/A	N/A	This is standard operating procedure for METOC data per OPNAV Instr 3140, 3500, and 5450 series.
	Collect, Process and distribute non-organic sensor info	N/A	No real sensors and no sensor management in ESG LOE.	Some success, but no standard procedures for distribution of info by either website or standard collaborations.	N/A	N/A	Excellent success using applications and reachback
	Provide precise navigation and time (PNT) to integrate weapons and sensors	N/A	No real sensors and no sensor management in ESG LOE.	Not addressed, but could reasonably be included in overall IM/KM info distribution.	N/A	N/A	N/A
Conduct distributed, collaborative command and control							
	Conduct battle management and C2 among Naval forces	Noted insufficient circuits to support adequate C2 on CHV and to support both C2 and MEU on USS *Essex*	No SOPs to establish C2 between ESG, STWC, and FFCC prior to STARTEX. ESG and FFCC targeting priorities and strike decision-making process were never well connected. FFCC largely acted autonomously.	Not well coordinated within IM/KM. Focus was primarily on chat, but there were significant shortcomings in this process (insufficient tools, multiple chat rooms, no time logs, etc.)	Voice SITREPS were basis for best SA. Deficiencies exist in user interfaces. Sneaker net still key to info transfers. Training weak in Fn technologies. Many calls for tech assist.	Highly successful in maintaining C2 linkages between ships using SATCOM and IBGWN, despite relatively high packet losses (20-30%) with IBGWN	N/A
	Conduct battle management and C2 with Joint forces	Similar implications as above, though not specifically discussed	Similar challenges to above.	Difficult:No standard chat program: Army uses IWS; Navy/MC uses IRC on IT21	N/A	Similar implications if ships are similarly equipped with IBGWN equipment	N/A
Provide dynamic, multi-path and survivable networks							

	Manage information transfer among Naval forces	Implication is that transfer is insufficient in that an accurate COP was not available.	Successfully communicated digital CFF with NFCS and to AFATDS. Did not demonstrate digital end-to-end capability only due to lack of digital interface with MK 86 GFCS.	Hardware functioned well; IM didn't to do as well.	No common links among fire support systems so process couldn't be automated	Highly successful	N/A
Function	**Sub-Functions**	**Command and Control**	**Fires**	**IM/KM**	**HSI**	**Technology**	**METOC**
	Manage information transfer with Joint forces	N/A	N/A	N/A	N/A	N/A	N/A
	Manage information transfer with civil / law enforcement agency networks	N/A	N/A	N/A	N/A	N/A	N/A
	Manage information transfer with Allied / Coalition forces	N/A	N/A	N/A	N/A	N/A	N/A
	Protect friendly information networks	N/A	N/A	N/A	N/A	N/A	N/A
	Establish networks with synchronized position and time	N/A	N/A	N/A	N/A	N/A	N/A
Provide adaptive and automated decision aids							
	Conduct operational and tactical planning	Confusion over roles and responsibilities. Most planning and execution over informal chat circuits.More training needed.	AFATDS with EMT/C2PC provided a real time projection of the forces ashore and made deconfliction successful.	IM/KM considerations were not incorporated into planning to the extent possible.	Good support to Fires process, but GCCS-M position data could lag up to 15 minutes, and SA was inaccurate after workarounds	N/A	Effectve qualitative, web-centric demonstration
	Conduct netted, prognostic logistics	N/A	N/A	N/A	N/A	N/A	N/A

Function	Sub-Functions	Command and Control	Fires	IM/KM	HSI	Technology	METOC
Organize, integrate and synchronize fires and maneuver to enable massed effects	Not discussed	Effects management tool provided accurate placements of battlespace geometries, target symbols, and fire support coordination measures.	N/A	Somewhat effective, but difficulties occurred in tracking critical events; resolving scheduling and resource conflicts; and universal understanding of SA.	N/A	N/A	
Provide human-centric integration	Dynamically allocate and control sensors and sensor platforms	N/A	N/A	N/A	Effective to a degree; not automated	N/A	N/A
	Provide tactically relevant and consistent environmental and PNT data to misssion planning and TDAs	N/A	N/A	N/A	N/A	N/A	Effective in qualitati sense. Ultimately needs to be extended automatic support t specific systems.
	Provide real-time adapatable man-machine forces	N/A	N/A	N/A	N/A	N/A	N/A
	Provide multi-linear cognitive processing warriors	N/A	N/A	N/A	N/A	N/A	N/A
	Protect friendly information outside the network	N/A	N/A	N/A	N/A	N/A	N/A
Provide information effects	Deny, degrade, and disrupt adversary information	N/A	N/A	N/A	N/A	N/A	N/A
	Influence adversary perception	N/A	N/A	N/A	N/A	N/A	N/A

Table 5. Trident Warrior 03 Results by FORCEnet Functional Capability[103]

[103] Trident Warrior 03 Summary Analysis Report, p. 11-14.

VI. CONCLUSIONS AND RECOMMENDATIONS

A. CONCLUSIONS AND RECOMMENDATIONS

As the military makes the transformation from the Industrial Age to the Information age, and continues its progress into the upper right hand quadrant of the transformation graph, it is apparent that "the network will be the single most important contributor to combat power."[104] This realization has led to the development of the NCW theory which segued into the Naval Services instantiation of it called FORCEnet. The Trident Warrior 03 exercise was then developed as a means to measure its success and to acquire data from which future exercises can be measured against. FORCEnet is still in its infancy and many people have different views on what exactly it is and how it should be implemented to achieve those goals. The intent of this thesis was not to answer those questions per se, but provide a realistic analysis of what worked during the TW03 exercise and what did not. This should provide a baseline for further Trident Warrior exercises so as to avoid the same mistakes in the future.

An important part of the process is to go back and look at the conceptual framework of the NCW model and relate specific examples from data that was collected from TW03 to examine the success of the exercise and to see how it holds up to the NCW domain model.

[104] Alberts, David and Hay, Richard. Power to the Edge: Command, Control in the Information Age, CCRP Publications, p.167.

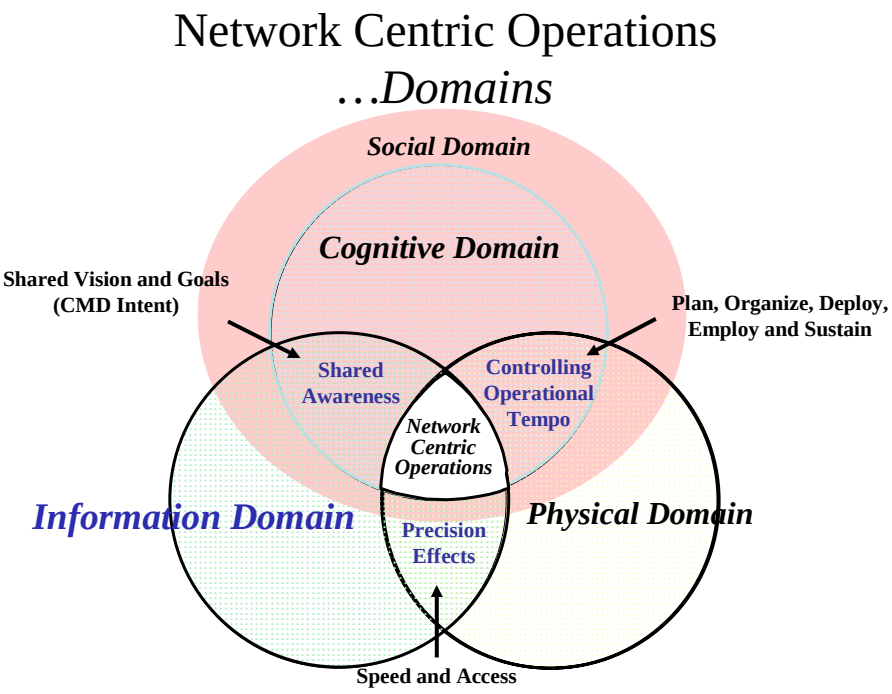


Figure 19. NCW Domain model[105]

1. Information Domain- is the figurative space where information resides and is transferred. The network is the main entity that allows participants to both push and pull information from the information domain. In TW03, the Automated Digital Network System (ADNS) was a revised routing architecture designed to take advantage of bandwidth increases and multiple satellite links with the application of router enhancements that would improve internet protocol (IP) traffic routing and packet delivery performance. Improvements made to the ADNS routing architecture had positive results on operational availability of IP networks supported. The updated routing architecture enabled mobile, self-forming networks among ships and across areas of responsibility (AORs), by modifying the autonomous system structure. The revised architecture leveraged commercial off-the-shelf (COTS) products in a configuration that allowed ADNS to adapt to the connectivity available to the units assigned.

The resulting network improved flexibility, survivability, and availability of warfighting networks without increasing the operator workload. As configured for the

[105]Holloman, Kim. Evidence Based Research Brief given at the NCO course at the Naval Post Graduate School, 15-18 July 2004

exercise, ADNS provided substantial increases in network availability and throughput. USS *Ft. McHenry*, for example, improved wide area network availability from 86% to 99.2%; throughput increased over 17%; outages were reduced by 91%; and the mean duration of outages dropped 74%. These technology advances are an essential component in the success of DoD's NCW capability. The following are recommendations to help improve the information domain.

Recommendations:

- Doctrine: Even as network outages decrease with improved technology, TTPs and policy will have to acknowledge that there will still be network outages and periods of reduced traffic flow.
- Organization: Afloat networking requires reorganization to mirror the way shore organizations support IP traffic flow. As new technologies emerge, the supporting infrastructure will have to adapt.
- Training: As more bandwidth is delivered to ships, the opportunity for remote training to equipment operators increased to the point where all post basic training should be accomplished onboard with the actual equipment and/or computer based training (CBT).
- Materiel: With the reliance on commercial off-the-shelf (COTS) networking equipment, the low cost of some devices has to be weighted against a potentially higher cost of making the equipment survivable in the warfighting maritime environment.
- Leadership: Leadership is required to merge the Naval networking visions with Joint requirements
- Personnel: As the quality of networking software improves the shipboard routers become easier to control and adapt from shore. Policy changes to allow for greater control of routers from ashore will affect shipboard manning practices.
- Facilities: If policy changes allowing shipboard router control are made in the future, then facilities will have to be modified ashore to support remote control of routers afloat.

2. Cognitive Domain- The cognitive domain states that an individual (or group) needs accurate and timely information to build situational awareness and understanding within the domain. In TW03 a common operational picture (COP) and shared situational awareness (SA) were not always possible which was a surprise given today's technology.

Gaps in shared situational awareness (SA) were observed. These included problems with the accuracy of the common operational picture (COP) and the ability for users to assess its validity, the inadequate management of air assets, and the deconfliction of airspace. Apparent causes included time latencies associated with the Global

Command and Control System-Maritime (GCCS-M), and connectivity and Concepts of Operations (CONOPs) for the ESG.

Effective collaboration in TW03 was limited due to a standard IRC chat program not being used between services. Independently, all such programs have some degree of inadequacy associated with them. Information management was available in a web portal but was not used, thus impacting the ability to move information from node to node, and limiting network-centric operations, as executed by the ESG. TW03 demonstrated that there are a number of hurdles to overcome before complex processes mature to the point where their use becomes commonplace. Additional work is needed to institutionalize concepts like the COP, asset management, deconfliction of airspace, and collaboration in order to rely confidently on them in battle. The following are recommendations to help improve the cognitive domain.

Recommendations:

- Organization: Evaluate and reorganize to institute collaborative technologies that are interoperable between all services.
- Training: Needs to be appropriate to the tasking in the ESG (which is more complex than an amphibious ready group (ARG)) and subordinate organizations.
- Leadership: Should be encouraged to examine processes and recommend improvements.

3. Physical Domain- is the tangible world of objects and actors. This shared understanding allows warfighters to make effective decisions in line with the plans and goals of the group than can be executed in the physical domain. In TW03 the digitizing and automating the Fires process end-to-end, from sensor to shooter improves the ESG's combat efficiency and effectiveness.

The Joint Fires network (JFN) on USS Blue Ridge provided digital intelligence, surveillance, and reconnaissance (ISR) data to the remote terminal capability (RTC) on USS Essex, which then provided digital target nominations to the Army Field Artillery Tactical Data System (AFATDS) and the Automated Deep Operations Coordination System (ADOCS), used by the Army (USA), Air Force (USAF) and Special Operations Forces (SOF). They in turn sent digital calls for fire (CFF) to the Naval Fires Control System (NFCS) on a missile platform (cruiser) which then simulated firing a weapon.

The value obtained from this was that it demonstrated inter-service connectivity and interoperability capabilities. Potential improvements to this process include:

- Faster reaction of Fires system through automation of information flow between system components.
- Automation of ESG reactions to targets and threats.
- Reduced human induced systems error (limiting humans in the loop activity of constantly having to re-insert targeting data e.g. coordinates).
- Improved situation awareness (SA) for all participants throughout the targeting process.
- Potential reductions in manpower due to increased automation of process. This is an implied result, as manpower impacts were not specifically tested over a range of conditions. In addition, addition of digital technology to the Fires process introduces requirements for addition technical support and watch stander expertise.

Recommendations:

- Doctrine: Develop Expeditionary Strike Group (ESG)/Strike Warfare Commander (STWC) Fires doctrine, including relationship to Joint doctrine.
- Organization: Additional experimentation needs to determine potential to streamline Fires organization and processes through introduction of digital technologies.
- Training: Training requirements need refinement in order to employ the digital and automated Fires process in the ESG. Current technology-watch stander configuration has single points of failure built in (e.g., a single technical support watch stander for all watches over a 24 hour period).
- Material: Current Fires network architecture is inconsistent set of system elements across Fleets. Standardization of an ESG Fires architecture would help to standardize material requirements. Evaluate opportunities for the design and acquisition of systems that can satisfy requirements of multiple Services and standardize the disparate processes.
- Personnel: Further experimentation needs to gather data to determine the "best fit" between technologies, mission requirements, and manpower under a range of conditions.

4. The Social Domain- is the intersection of people living and working together, either in person or through a network. The aggregation of synchronized actors creates a virtual team in the social domain that works together toward common ends. In TW03 this was the area that needed the most work and was the weakest link in the domain model.

TW03 had only five days dedicated to the experiment, so that there was limited opportunity for participants learn how to incorporate new technical capabilities into normal tasks. The learning curve was steep in some cases, and a steady-state performance was not attained. With additional time, these limitations would likely have been overcome. Also, there were conflicting priorities between TW03 objectives and the concurrently scheduled Special Operations Capability Certification Exercise (SOCCEX). This presented a time challenge to complete the data collection requirements.

Recommendation:

The biggest recommendation to help improve the social domain is that there needs to be a clear, concise plan and objectives that need to met in a dedicated exercise format. It is hard to test an experiment that is tacked on the back end of another experiment (SOCCEX). If there is no dedication to the experiment, then the data that is collected is not as valuable as it would be under more dedicated circumstances

In summary, technologically, the U.S. military forces are more advanced today than any other military force in the world. However, if the U.S. wants to be a fully functioning NCW force, it needs to work in harmony with all four domains of the conceptual framework. To be exceptional in one domain and be weak in others will not compensate. All the domains must be focused on so that there can be a synergy between the commander and his forces.

B. AREAS FOR FURTHER RESEARCH

During the course of this research, the author crossed the boundaries of many exciting and innovating topics that are ripe for exploration. Some of the areas in need of further research are:

- Continued evaluation of the Trident Warrior Exercises. The evaluation could focus on the technological side, the operational side or the organizational side.
- A huge obstacle to interoperability is in the Social Domain. There could be a comprehensive thesis on how to break through cultural and bureaucratic barriers in the U.S. military.

- The Air Force has its own version of FORCEnet called Constellation. Will it be interoperable with the other services and what do their exercises look like to measure its stated assumptions. The same goes for the Army's version of FORCEnet called LANDWARNET.
- A major issue in the software engineering field is taking a look at the FORCEnet architecture and evaluating it. How close is the Naval Services to a truly integrated and interoperable force?

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Adkins, Mark and Kruse, John. University of Arizona Case Study: Network Centric Warfare in the U.S. Navy Fifth Fleet. August 3, 2003.

Admiral Vern Clark, Sea Power 21. Proceedings, October 2002.

Alberts, David S and Hayes, Richard E., Power to the Edge: Command, Control in the Information Age, Department of Defense C4ISR Cooperative Research Program, June 2003.

Alberts, David S. and Gartska, John J., and Stein, Fred P., *Network Centric Warfare: Developing and leveraging Information Superiority*, Department of Defense C4ISR Cooperative Research Program, 1999.

Alberts, David S. Information AgeTransformation: Getting To A 21stCenturyMilitary, Department of Defense C4ISR Cooperative Research Program, June 2002.

Arquilla, John and Rondeldt, David, In Athena's Camp: Preparing for Conflict in the Information Age, Rand Publications, 1997.

Battle Speed. Washington Times. April 7, 2003.

Berkowitz, Bruce, The New Face of War: How War Will Be Fought in the 21st Century, The Free Press, 2003.

Bowden, Scott. Forward Presence, Power Projection, and the Navy's Littoral Strategy: Foundations, Problems and Prospects.

Chief of Naval Operations (CNO) Strategic Studies Group (SSG) XIX, *Naval Power Forward*, September 2000.

Chief of Naval Operations (CNO) Strategic Studies Group (SSG) XX, *FORCEnet and the 21st Century Warrior*, November 2001.

Clark, Vern. Sea Power 21, Part I. U.S. Naval Institute Proceedings, October 2002.

Defense Information Systems Agency http://www.disa.mil/main/prodsol/gig_be.html visited July 31st, 2004

Evans, Nicholas D. Military Gadgets: How Advanced Technology Is Transforming Today's Battlefield...and Tomorrow's.

Fleet Battle Experiment–Kilo Network Analysis. Naval Postgraduate School. May 2003.

Gallup, Shelley. Interview with author. July 16, 2004.

Hesser, Woodrow and Rieken, Danny. FORCEnet Engagement Packs: "Operationalizing" FORCEnet to Deliver Tomorrow's Naval Network-Centric Combat Reach Capabilities...Today. December 2003.

Holloman, Kim. Evidenced Based Research given at a NCO course at the Naval Postgraduate School, 15-18 July 2004.

IRIS Independent Research Website www.irisresearch.com/littorals.htm. visited July 31, 2004.

Joint Publication 1-02, Department of Defense Dictionary of Military and Associated terms, 12 April 2001.

Joint Publication 3-13, Joint Doctrine For Information Operations, 09 October 1998

Joint Vision 2020: America's Military Preparing for Tomorrow

Mackercher, John. We Have More to Learn from Iraqi Freedom, Proceedings. August 2004.

Naval Operating Concept for Joint Operations, www.mccdc.usmc.mil visited 31 July 2004.

NCW Primer CD-ROM. Network Centric Operations: Understanding the Emerging Information Age Force. Conference at the Naval Postgraduate School, Monterey, California, July 12-15, 2004.

Network Centric Operations: Understanding the Emerging Information Age Force. Conference at the Naval Postgraduate School, Monterey, California, July 12-15, 2004.

Roche, Patrick. A FORCEnet Framework for Analysis of Existing Naval C4I Architectures. Master's Thesis, Naval Postgraduate School, Monterey, California, June 2003.

Trident Warrior 03 Summary Analysis Report, Naval Network Warfare Command, Norfolk, VA.

Zinni, Anthony USMC General (ret) Interview on Transformation 17 June 2004.

APPENDIX INTERVIEW WITH GENERAL ZINNI ON TRANSFORMATION

17 June 2004

1. What are the General's thoughts on "Transformation" and whether going to a smaller, mobile, military is the right approach?

General Zinni stated that the military transformation process was "ill-defined" and that there needs to be major changes to its existing structure. There were three main areas that he said needed to be addressed:

1. The first thing that the US needs to do in its reformation process is rethink our staffing of personnel in the military. General Zinni stated that the US needs to look at the time in grade and promotion levels of our officers and enlisted troops. The General believes that there shouldn't be a blanket "up and out" policy for our troops and that longer time in grade or service should actually be encouraged. He said that we were losing a wealth of knowledge when we engage in such practices and that many personnel who are forced out after 20 years of service take their highly valued education and training with them when they still could be of value to the military. The General also stated that we should spend more in investing in our troop's education and schooling. Future combat soldiers will need to be well versed in global politics and economics besides their military occupational specialties (mos).
2. The second main topic that was addressed was our "continuing in modernization" of our military forces. The US should continue its exploitation of stealth missiles and laser guided technology. In doing so would also require the US to do away with its "cold war" era of the acquisition process. With the advancement of technology moving at the speed of Moore's law we can no longer have programs that take 5 to 10 years to get through the acquisition cycle. When it comes to Information Technology (IT) the Military needs to make sure that the systems are integrated with each other and that there are standards and architecture in place in place before the purchase. We can no longer invest in stovepipe or legacy systems.

   The US needs to move away from antiquated capabilities and doctrine such as the use of land mines. The politics of using such doctrine does not put the US military in a positive light. The General stated that we could replace such doctrine with alternative non-lethal technology. Technology that isn't as devastating or as long lasting.
3. The third area that the General noted is the need to redesign our force structure. It is too costly to have large formations of troops when the focus should be on smaller security forces that focus on peace-keeping and

civil affairs. The US needs to concentrate on training for security missions and develop technology for urban warfare. One example General Zinni gave was how the British forces redesigned their units in Northern Ireland to focus on combating terrorist type activities.

2. Is change possible with the culture of leadership that is present in today's Marine Corps?

The Marine Corps needs problems solvers who are flexible and adaptable in an ever changing environment. General Zinni reiterated that the Marine Corps should focus on schooling and training so Marine leaders can be able decision makers. One example that General Zinni gave on organizational structure was when his MEF staff organized the unit like a trucking company. A good trucking company needs to process information quickly if it is going to stay ahead of its competitors and the General wanted his staff to think in the same manner. General Zinni also noted that there needs to be the existence of a Command and Control expert and an IT specialist to a unit.

3. Does the transformation process include the emergence of Special Operating Forces (SOF)?

The General noted the SOF's are similar to a "one-stop shopping" where everything is brought together under one command. This requires greater education and training as well as longer time in service to create these specialists. General Zinni finished the interview by stating that a much needed requirement for our future leaders is the study of foreign cultures to help with the coalition building process. He went on to say that Foreign Area Officers (FAO) are worth their weight in gold in the planning process and their knowledge needs to be cultivated to the maximum extent possible. As a plug for the Naval Postgraduate School, he stated that promotion boards should not hold schooling against an individual in the promotion process but realize the benefits it has to offer the Marine Corps in the long run and build on it.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Dan C. Boger
   Naval Post Graduate School
   Monterey, California

4. Sue Higgins
   Naval Postgraduate School
   Monterey, California